California Privacy and Security Advisory Board

INTERIM PRIVACY AND SECURITY GUIDELINES

HEALTH INFORMATION EXCHANGE (HIE)

IN CALIFORNIA

Version	Date	Description
1 & 2	Aug09 – Oct09	The Guidelines were completed as separate parts (privacy & security) and vetted as versions 1 & 2 at different dates.
3	Oct 16 2009	Posted for 30 day public comment.

TABLE OF CONTENTS

1.0 GENERAL PROVISIONS

1.1 PURPOSE

The purpose of the Privacy and Security Guidelines is to safeguard patients' individual health information while facilitating the sharing of such information to improve the quality of health care.

1.2 CALIFORNIA PRIVACY AND SECURITY ADVISORY BOARD GUIDANCE

Entities shall operate within the California Privacy and Security Advisory Board vision and principles adopted by the California Health and Human Services Agency.

1.2.1 Vision	The vision is to enable the electronic transfer of individual health information to improve the quality of care in a way that fosters trust.
1.2.2. Mission of the Guidelines	The mission of these guidelines is to respect the privacy and security of personal health information, enhance trust, and promote quality of care.
1.2.3 Assumptions	The principles assume that: (a) Improved quality of care is the most important objective of electronic health information exchange. Other considerations may include: healthcare operations, public health, research, health care oversight, and payment. (b) Entities shall utilize the minimum necessary in collection, use, disclosure, storage, and retention of health information as appropriate to protect individuals. Consideration: Entities shall use anonymized data when practicable.
1.2.4 Principles	The following principles shall provide foundational framework for the guidelines to balance individual privacy with the potential benefit that electronic health information exchange provides to the quality of care for an individual.
Openness	There shall be a general policy of openness among entities that participate in electronic health information exchange about developments, practices, and policies with respect to individual health information.
Individual Health Information Quality	Health information shall be relevant, accurate, complete, and kept up-to-date**.**
Individual Participation	Individuals have the right to: a. Ascertain the person responsible for individual health information for an entity, obtain confirmation of whether the entity has specific

	individual health information relating to the individual, and obtain its location. b. Receive their individual health information in a reasonable time and manner, at a reasonable charge, and in a format that is generally accessible by individuals. c. Challenge the accuracy of their individual health information and, if successful, to have the individual health information corrected, completed, or amended. d. Control the access, use, or disclosure of their individual health information, unless otherwise specified by law or regulation.
Collection Limitation	There shall be limits to the collection of individual health information. Individual health information shall be obtained by lawful and fair means. Where appropriate, it shall be obtained with the knowledge or consent of the individual. The specific purposes for which individual health information is collected shall be specified not later than at the time of collection.
Individual Health Information Limitation	Use and disclosure of individual health information shall be limited to the specified purpose. Certain use and disclosure shall require consent.
Purpose Limitation	Individual health information shall be relevant to the purpose for which it is to be used and, limited to the minimum information necessary for the specified purpose. The subsequent use shall be limited to the specified purpose.
De-Identified Information	De-identified individual health information shall not be re-identified unless specified in law. If de-identified individual health information is re-identified, it shall be subject to these principles. De-identified individual health information shall not be disclosed if there is a reasonable basis to believe that the information can be used to identify an individual.
Security Safeguards	Individual health information shall be protected by appropriate security safeguards against such risks as loss or destruction, unauthorized access, use, modification or disclosure of data.
Accountability	An entity shall comply with laws, regulations, standards, and organizational policies for the protection, retention, and destruction of individual health information. Any person who has access to individual health information shall comply with those provisions.

1.3 SCOPE

The guidelines shall apply to individual health information in any form accessed, licensed, stored, transmitted, or maintained, except for individual health information that has not been accessed or

transmitted on or after the effective date of the guidelines. An entity that has not electronically accessed, transmitted, or received individual health information is not subject to these guidelines until the date on which it begins accessing, transmitting or receiving individual health information electronically.

1.4 APPLICABILITY

Entities in California who receive federal American Recovery and Reinvestment Act of 2009, Health Information Technology for Economic and Clinical Health (HITECH) funding received through the California State Health and Human Services Agency shall comply with these guidelines.

Such entities shall comply with amendments required by future HITECH regulations, State law, and amendments to these Guidelines, as appropriate.

1.4.1 Personal Representative	An entity shall treat a person as an personal representative when they are: (a) A parent or guardian of a minor who is a patient, (b) Conservators, guardians, or agents *(pursuant to Probate Code § 4607)* of a person or adult patient, or (c) The executor, administrator, beneficiary *(as defined in Section 24 of the Probate Code or personal representative as defined in Section 58 of the Probate Code)*, or personal representative of a deceased person. An entity shall not treat a person as a personal representative when an individual is an emancipated minor, in situations with unemancipated minors described below *(Section 1.4.2)*, and for individuals in specified abuse, neglect or endangerment situations *(described in Section 2.3, Patient Access)*. *[References:* 45 C.F.R. *§ 164.502(g), California Health and Safety Code § 123105(e) and 123110(a)]*
1.4.2 Adult or Emancipated Minors	An entity shall treat as an "individual" a person who has authority to act on behalf of an individual who is an adult or an emancipated minor with respect to making decisions related to health care relevant to such representation. *[Reference: 45 C.F.R. § 164.502(g)(2)]*
1.4.3 Unemancipated Minors	An entity shall treat as a "personal representative" a parent, guardian, or caregiver who has authority to act on behalf of an unemancipated minor, with respect to making decisions related to health care relevant to such personal representation. Such person may not be a personal representative of an unemancipated minor when: (a) The minor has the right to control their individual health information. (b) The minor lawfully obtained such heath care services without the consent of a parent, guardian, or other person acting in loco parentis, and the minor, a court, or another person authorized by law consents to such health care

	services, or (c) A parent, guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a health care provider and the minor with respect to health care services. *[Reference: 45 C.F.R. § 164.502(g)(3)(i)]*
1.4.4 Minor's Control of Individual Health Information	A minor may control their information, as authorized by law to consent for treatment, when: (a) Aged 15 or older and consented for medical care when living separately from their parents and managing their own financial affairs. *[California Family Code § 6922]* (b) A minor consented to receive his/her own health care when: (i) The minor is 12 years of age or older, seeks or receives mental health treatment or counseling on an outpatient basis, or from a residential shelter service. *[California Family Code § 6924(b)]* (ii) The minor seeks pregnant care or prevention of pregnancy. *[California Family Code § 6925]* (iii) The minor, 12 years of age or older, may have come in contact with infectious, contagious, sexually transmitted disease or communicable diseases required to be reported to health care officers. *[California Family Code § 6926]* (iv) The minor, 12 years of age or older, alleges rape. *[California Family Code § 6927]* (v) The minor alleges to have been sexually assaulted. *[California Family Code § 6928]* (vi) The minor, 12 years of age or older, seeks care for drug or alcohol related problems. *[California Family Code § 6929(b)]*
1.4.5 Unemancipated Minors – Exceptions	A parent, guardian, or other person acting *in loco parentis* is the personal representative and has the right to control information of an unemancipated minor, except: (a) When the minor has the right to control his/her own information pursuant to section 1.4.4 above; (b) The parent, guardian or other person acting *in loco parentis* assents to an agreement of confidentiality between the health care provider and the minor with respect to specific health care services; or (c) The health care provider, in the exercise of professional judgment, determines that access to the records by the personal representative would have a detrimental effect on the provider's professional relationship with the minor patient or on the minor's physical safety or psychological well-being. *[References: California Health & Safety Code section 123115(a) and 45 C.F.R. § 164.502(g)(3)(i)(C)]*

1.4.7 Deceased	An entity shall treat an executor, administrator, beneficiary, or other person with legal authority to act on behalf of a deceased individual or of the individual's estate, as a personal representative with respect to individual health information relevant to such personal representation. *[References: 45 C.F.R. § 164.502(g)(4), Health and Safety Code § 123105(e), & Health and Safety Code § 123105(e) and 123110(a)]*

2.0 INDIVIDUAL RIGHTS	
	An individual has specific rights regarding their individual health information held by an entity. An entity shall ensure that an individual participating in an electronic health information exchange has the opportunity to: (a) Ascertain who the person is that is responsible for his/her individual health information within the entity or contact information for other entities with which the entity exchanges the individual's information, (b) Obtain confirmation of whether the entity is in custody of or controls his/her individual health information, (c) Obtain the location of the individual health information, (d) Receive his/her individual health information in a reasonable time and manner, at a reasonable charge, and in a format that is accessible and meet these guidelines *(see section 2.4),* (e) Challenge the accuracy of his/her individual health information with the possibility of correction, completion, or amendment *(see section 2.6),* and (f) Control the access, use, or disclosure of their individual health information as specified in these guidelines *(see section 2.1)*. *[References: California Privacy and Security Advisory Board Principle 3 – Individual Participation, Principle 6 – Purpose Limitation;* *Consent references – 12/28/2000 45 CRF Parts 160 and 164; 45 C.F.R. § 164.524* *Access of individuals to protected health information, § 164.526 Amendment of protected health information, § 164.528 Accounting of disclosures of protected health information, § 164.522* *Rights to request privacy protection for protected health information; § 164.502(g)(1)* *Personal Representatives; Patients Access to Health Records Act (PAHRA) in the Health and Safety Code, Sections 123100 et seq.; Information Practices Act (IPA) CA Civil Code Section 1798.32 – 1798.34; IPA CA Civil Code section 1798.24(c); IPA CA Civil Code section 1798.35; Confidentiality of Medical Information Act (CMIA) CA Civil Code Section 56.07; CMIA CA Civil Code Section 56.11 & 56.12; Welfare and Institutions Code Section 5010; ARRA Sections 13405(a)* *Requested Restrictions on Certain Disclosures of Health Information, 13405(c)* *Accounting of Certain Protected Health Information Disclosures Required if Entity Uses Electronic Health Record, 13405(e) Access to Certain Information in Electronic Format*

2.1 HIECONSENT	
2.1.1 Individual Choice to Participate	An individual has the right to choose to restrict or enable his/her individual health information to be exchanged through an electronic health information exchange as provided below.
2.1.1.1 OPT OUT FOR CLINICAL TREATMENT PURPOSES	An individual may opt out of having his/her individual health information, transmitted through an electronic health information exchange for purposes of clinical treatment when a treatment relationship exists. A clinical treatment relationship exists when there is interaction between: (a) An individual and a health care provider who delivers treatment to the individual, (b) The primary health care provider who delivers the original health care to the individual and the secondary health care provider who delivers additional health care services based on the orders of the primary health care provider, or (c) Health care providers who are members of a multi-disciplinary team and an individual for the diagnosis and treatment of that individual. *[Based on the definition of indirect treatment relationship in 45 CFR § 164.501]*
2.1.1.2 NO CONSENT IN EMERGENCY SITUATIONS	An entity may transmit through an electronic health information exchange individual health information for purposes of clinical treatment without the individual's consent when the individual in incapable of making a choice concerning the transmission of his/her health information when: (a) It is in the individual's best interest as determined by a health care provider, in the exercise of professional judgment, (b) It is consistent with prior preferences of the individual. The entity must inform the individual and provide an opportunity to opt out of having his/her health information transmitted electronically for purposes of clinical treatment when it becomes practicable to do so.
2.1.1.3 NO CONSENT FOR MANDATED PUBLIC HEALTH	An entity may transmit through an electronic health information exchange individual health information for public health purposes for which the law requires the disclosure of the information. *(See Appendix A for a non-inclusive listing of laws pertaining to public health purposes.)*
2.1.1.4 OPT IN FOR - SENSITIVE INFORMATION	An entity shall not transmit sensitive individual health information through an electronic health information exchange if the disclosure of the sensitive individual health information is otherwise restricted by law unless the entity has obtained from the individual who is subject of the sensitive individual explicit documented consent to have his/her information exchanged electronically before it is transmitted.

2.1.1.5 OPT IN FOR OTHER PURPOSES	An entity shall obtain from an individual an explicit documented consent to have his/her individual health information, including individual sensitive health information, transmitted through an electronic health information exchange prior to the transmission: (a) For all other purposes for use and disclosure of an individual's health information other than clinical treatment *(Section 2.1.1.1)* or mandated public health *(Section 2.1.1.2)*.
2.1.1.6 LIMITED BY USES AND DISCLOSURES	An individual's documented consent to have his/her health information transmitted through an electronic health information exchange shall be limited to the purposes of uses and disclosures of individual health information as permitted under these guidelines *(see Section 3.2)*. *[45 C.F.R. Part 160, 162, and 164 and California Civil Code § 56 et seq., California Privacy and Security Advisory Board Principles 3, Individual Rights.]*
2.1.3 Minors as Individuals	An entity shall obtain the appropriate HIEconsent from a minor when a minor is considered an individual. In such circumstances, an entity shall not seek HIEconsent from the parent or personal representative of the minor unless permitted by the minor. *(See section 1.4.4 for situations where a minor is considered an individual.)*
2.1.4 Informing Individuals of HIEconsent	An entity shall inform the individual that he/she: (a) Does not have the right to restrict or enable the transmission of his/her individual health information through an electronic health information exchange when the purpose for the use or disclosure of the individual health information is required by law. (b) Has the opportunity to restrict or enable transmission of his/her individual health information through an electronic health information exchange. (i) Has the right to opt out of transmitting his/her individual health information through an electronic health information exchange for purposes of clinical treatment between providers who have a treatment relationship with the individual. However, in situations where the individual is not capable of making a decision *(such as in an emergency where the individual is unconscious)* concerning the transmission of his/her individual health information through an electronic health information exchange, it may be transmitted at the discretion of the treating provider. (ii) Has the right to opt into transmitting his/her sensitive information through an electronic health information exchange, unless otherwise required by law. (iii) Has the right to opt into transmitting his/her individual health information through an electronic health information exchange for all other purposes permitted under these guidelines.

2.1.4.1 HIECONSENT NOTICE	An entity shall facilitate knowledgeable HIEconsent by providing the individual a separate notice that contains the following statements:
NO CONSENT STATEMENT	The entity will be transmitting the individual's health information through an electronic health information exchange without consent from the individual if the disclosure is required by law, including for public health purposes.
OPT OUT STATEMENT	The individual's health information will be transmitted through an electronic health information exchange to other health care providers for the purposes of clinical treatment where a treatment relationship exists between the providers and the individual when: (a) The individual has been successfully informed that he/she has the choice to opt out of having his/her information exchanged for this purpose, (b) The individual has been notified of how the individual may opt out of having his/her health information for purposes of treatment between providers with a direct treatment relationship with the individual, and (c) 30 days have elapsed in which the individual could respond to the notification, or (d) The individual has responded that he/she chooses not to opt out of having his/her individual health information transmitted through an electronic health information exchange.
OPT IN STATEMENT	The individual may opt into his/her sensitive health information being transmitted through an electronic health information exchange where allowed by law, or The individual may opt into his/her health information being transmitted through an electronic health information exchange for all other purposes permitted under these guidelines other than clinical treatment where a relationship between the individual and health care providers exist or for mandated public health purposes; when: (a) The individual has been notified of how the individual may opt into having his/her health information transmitted through an electronic health information exchange and has agreed to such transmissions.
OTHER STATEMENTS	(a) A general description of the benefits and risks associated with including or not including an individual's health information for exchange through an electronic health information exchange. (b) A list of the benefits and risks associated with including or not including an individual's sensitive health information for exchange through an electronic health information exchange. (c) A statement that the individual may revoke his/her choice to include or exclude his/her individual health information from transmission through an electronic health information exchange at any time and how and

	when that action will be effective. (d) A statement that revocations of his/her choice to include or exclude his/her information from transmission through an electronic health information exchange will not remove his/her previously exchanged health information from the health information exchange, but will prevent further exchange or transmission . *[Reference: New York State HIE Policies, Canada Personal Health Information Protection Act]*
2.1.5 Revocation of HIEconsent Decision	An individual has the right to revoke. An entity shall make the individual health information unavailable to be transmitted through an electronic health information exchange when an individual: (a) Revokes his/her choice to opt out of having his/her individual health information transmitted through an electronic health information exchange for clinical treatment purposes, or (b) Revokes his/her choice to opt into having his/her sensitive health information transmitted through an electronic health information exchange of his/her and individual health information, or (c) Revokes her/her choice to opt into having his/her individual health information exchanged for other purposes permitted under these guidelines.
2.1.6 Individual Health Information Available for Transmission	The individual health information shall be available for transmission through an electronic health information exchange when: (a) An individual does not respond to the notification of his/her right to opt out of transmitting his/her individual health information through an electronic health information exchange within 30 days, (b) An individual provides HIEconsent to transmit his/her sensitive individual health information through an electronic health information exchange, or (c) An individual provides HIEconsent to transmit his/her individual health information through an electronic health information exchange for other purposes permitted under these guidelines.
2.1.7 Applicability of a Revocation	A revocation of HIEconsent does not apply to individual health information exchanged prior to the revocation or to exchanges of individual health information mandated by law for public health purposes.
2.1.8 Resolving Conflicting HIEconsents	Entities, in consultation with the individual and/or the entities with whom the conflict exists, shall have a mechanism to identify and address conflicts concerning the transmission of individual health information through an electronic health information exchange. *[Reference:45 C.F.R. § 164.508]*
2.1.9 Federal and State Laws	An individual's choice to include or exclude his/her individual health information from transmission through an electronic health information exchange shall not be construed to waive any privilege granted under

	federal, state, or local law or procedure. *[Reference: § 164.506 preamble discussion, October 2000 Final Regulations]*
2.1.10 Conditional Treatment	An entity may not condition treatment, payment, enrollment, or eligibility for benefits on: (a) Whether the individual chooses to opt out of transmitting his/her individual health information electronically through a health information exchange for purposes of clinical treatment among providers who have a treatment relationship with the individual. (b) Whether the individual does or does not consent to his/her individual health information transmitted electronically through a health information exchange outside of the entity for all other purposes permitted under these guidelines. (c) Whether the individual does or does not consent to his/her sensitive health information transmitted electronically through a health information exchange. *[Reference: Consistent with 45 C.F.R. § 164.508(c)(2)]*

2.2 RIGHT TO NOTICE OF PRIVACY PRACTICES

An individual has a right to adequate notice of the uses and disclosures of individual health information that may be made by an entity, the individual's rights, and the entity's legal duties with respect to individual health information.

2.2.1 Exceptions	An entity is not required to provide a notice of privacy practices when:
2.2.1.1 EXCEPTION FOR GROUP HEALTH PLANS	Exceptions for group health plans: (a) An individual is enrolled in a group health plan and receives a notice: (i) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or (ii) From the health insurance issuer or HMO with respect to the group health plan through which such individuals receive their health benefits under the group health plan. (b) When a group health plan: (i) Provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and (ii) Creates or receives individual health information in addition to summary health information or information on whether the individual is participating in the group health plan, or (iii) Is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, The group health plan must: maintain a notice under this section; and provide such notice upon request to any person. The provisions of the notice do not apply to such group health plan. (c) A group health plan: (i) Provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and (ii) Does not create or receive individual health information other than summary health information or information on whether an individual is participating in the group health plan, or (iii) Is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan. Such health plan is not required to maintain or provide a notice under this section. *[Reference: 45 C.F.R. § 164.520(a)(2)]*
2.2.1.2 EXCEPTION FOR INMATES	An inmate does not have a right to notice under this section, and the requirements of this section do not apply to a correctional institution.

	[Reference: 45 C.F.R. § 164.520(a)(3)]
2.2.2 Adequate Notice and Content of Notice – Required Elements	A notice shall be considered adequate when it meets the following requirements. An entity shall provide a notice that is written in plain language and that contains the following elements. *[Reference: 45 C.F.R. § 164.520 & 45 C.F.R. § 164.520(b)(1)]*
2.2.2.1 NOTICE HEADER	The notice shall contain the following statement as a header or otherwise prominently displayed: "THIS NOTICE DESCRIBES HOW HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY." *[Reference: 45 C.F.R. § 164.520(b)(1(i))]*
2.2.2.2 USES AND DISCLOSURES	The notice shall contain: (a) A description, including at least one example, of each type of use and disclosure of individual health information that the entity is permitted to make for each of the following purposes: treatment, payment, and health care operations. (b) A description of each of the other purposes for which the entity is permitted or required to use or disclose individual health information without the individual's written authorization. (c) If a use or disclosure for any purpose is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law. (d) The description of the uses and disclosures must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required. (e) A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization. (f) A statement that uses and disclosures of individual health information, in a health information exchange, for treatment purposes, will be made only with the individual's written HIEconsent for sensitive individual health. *[Reference: 45 C.F.R. § 164.520(b)(1)(i)(E), 164.506(c), & New York State HIE Policies]*
2.2.2.3 SEPARATE STATEMENTS FOR CERTAIN USES AND DISCLOSURES	If an entity intends to engage in the following activity, the description must include a separate statement, as applicable, that: (a) If the entity has a direct treatment relationship it may contact the individual to provide appointment reminders or information about current treatment; or

	(b) If the entity is a health plan, it may describe a health-related product or service(or payment for such product or service) that is provided by, or included in a plan of benefits of, the health plan making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits. *[Reference: 45 C.F.R. 164.501 definition of Marketing, paragraph (1) & C.F.R. § 164.520(b)(1)(iii), Civil Code 56.10(a)]*
2.2.2.4 INDIVIDUAL RIGHTS	The notice shall contain a statement of the individual's rights with respect to individual health information and a brief description of how the individual may exercise these rights, as follows:
2.2.2.5 RESTRICTIONS	The right to request restrictions on certain uses and disclosures of individual health information, including a statement that the entity is not required to agree to a requested restriction except for requested restrictions where the individual paid for services out of pocket and requests to restrict the disclosure of their individual health information to health plans for payment and/or health care operation purposes,
2.2.2.6 CONFIDENTIAL COMMUNICATIONS	The right to receive confidential communications of individual health information as applicable (*see Section 2.5*), *[Reference: 45 C.F.R. § 164.522(b)]*
2.2.2.7 COPIES	The right to inspect and copy individual health information. (*See Section 2.4)*, *[Reference: 45 C.F.R. § 164.520(b)(1)(iv)(C)]*
2.2.2.8 AMENDMENTS	The right to amend individual health information, *(See Section 2.6.4).* *[Reference: 45 C.F.R. § 164.526(a)]*
2.2.2.9 ACCOUNTING OF DISCLOSURES	The right to receive an accounting of disclosures of individual health information and the period for which the accounting may cover *(See Section 2.7)*. *[Reference: 45 C.F.R. § 164.528]*
2.2.2.10 COPY OF NOTICE	The right of an individual, including an individual who has agreed to receive the notice, to obtain a paper or electronic copy of the notice from the entity upon request, *[Reference: 45 C.F.R. § 164.520(b)(1)(iv)(F)]*
2.2.2.11 HIECONSENT OPTIONS	The right of the individual to be informed about his/her HIEconsent options *(See Section 2.1),*

2.2.2.12 EXPLANATION OF NOTICE	The right of the individual to have the notice of privacy practices explained prior to his/her signing the HIEconsent form *(See Section 2.1)*. *[Reference: New York State HIE Policies]*
2.2.2.13 ENTITY'S POLICIES	A statement that the entity is to maintain the privacy of individual health iformation and to provide individuals with notice of its duties and privacy practices with respect to individual health information,
2.2.2.14 TERMS OF NOTICE	A statement that the entity is required to abide by the terms of the notice currently in effect, and
2.2.2.15 REVISIONS TO NOTICE	For an entity to apply a revision in a privacy practice that is described in the notice to individual health information that the entity created or received prior to issuing a revised notice, a statement that the entity reserves the right to change the terms of its notice and to make the new notice provisions effective for all individual health information that it maintains. The statement must also describe how it will provide individuals with a revised notice. *[Reference: 45 C.F.R. § 164.520(b)(1)(v)]*
2.2.2.16 COMPLAINTS	The notice shall contain a statement that individuals may complain to the entity, and to the Secretary of the U.S. Department of Health and Human Services if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with the entity, and the Secretary of the U.S. Department of Health and Human Services, and a statement that the individual will not be retaliated against for filing a complaint. *[Reference: 45 C.F.R. § 164.520(b)(1)(vi)]*
2.2.2.17 CONTACT	The notice shall contain the name, or title, and telephone number of a person or office to contact for further information. *[Reference: 45 C.F.R. § 164.520(b)(1)(vii)]*
2.2.2.18 EFFECTIVE DATE	The notice must contain the date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published. *[Reference: 45 C.F.R. § 164.520(b)(1)(viii)]*
2.2.2.19 OPTIONAL ELEMENTS.	If an entity elects to limit the uses or disclosures that it is permitted to make, the entity:: (a) May describe its more limited uses or disclosures in its notice, and (b) Does not include in its notice a limitation affecting its right to make a use or disclosure that is: (i) Required by law or (ii) Necessary to prevent or lessen a serious or imminent threat to the health and safety of a person or the public. (c) For an entity to apply a change to a notice of limited uses and

	disclosures of individual health information created or received prior to issuing a revised notice: (i) The notice must include the statements required above for an entity's duties regarding changing a notice.
2.2.3 Revisions to the Notice	The entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the entity's duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected. *[Reference: 45 C.F.R. § 164.520(b)(2)(ii)]*
2.2.4 Provision of Notice	An entity must make the notice available on request to any person and to individuals, as applicable, and as follows: *[Reference: 45 C.F.R. § 164.520(c)]*
2.2.5 Specific Requirements for Health Plans	A health plan must provide notice: (a) At the time of enrollment, to individuals who are new enrollees, and (b) Within 60 days of a material revision to the notice, to individuals then covered by the plan, (c) No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice, (d) The health plan satisfies the requirements of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents, and (e) If a health plan has more than one notice, it satisfies the requirements of this section by providing the notice that is relevant to the individual or other person requesting the notice. *[Reference: 45 C.F.R. § 164.520(c)(1)]*
2.2.6 Specific Requirements for Certain Health Care Providers	An entity that has a direct treatment relationship with an individual shall: (a) Provide the notice: (i) No later than the date of the first service delivery, including service delivered electronically, to such individual or (ii) In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation. (b) Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained; (c) If the health care provider maintains a physical service delivery site: (i) Have the notice available at the service delivery site for

	individuals to request to take with them; and (ii) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the health care provider to be able to read the notice; and (d) Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of this section, if applicable. *[Reference: 45 C.F.R. § 164.520(c)(2)]*
2.2.7 Specific Requirements for Electronic Notice	(a) An entity that maintains a web site that provides information about the entity's customer services or benefits shall prominently post its notice on the web site and make the notice available electronically through the web site. (b) An entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the entity will satisfy the provision requirements this section when made timely in accordance this section. (c) If the first service delivery to an individual is delivered electronically, the health care provider must provide electronic notice automatically and contemporaneously in response to the individual's first request for service. The requirements for providing a notice in an emergency situation apply to electronic notice. (d) The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from an entity upon request. *[Reference: 45 C.F.R. § 164.520(c)(3)]*
2.2.8 Joint Notice by Separate Entities	Entities that participate in a Health Insurance Portability and Accountability Act (HIPAA) defined organized health care arrangements may comply with this section by a joint notice, provided that: (a) The entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to individual health information collected, created, requested or received by the entity as part of its participation in the organized health care arrangement; (b) The joint notice meets the requirements of this section, except that the statements required by this section may be altered to reflect the fact that the notice covers more than one entity; and (i) Describes with reasonable specificity the entities, or class of entities, to which the joint notice applies; (ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and

	(iii) If applicable, states that the entities participating in the organized health care arrangement will share individual health information with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement. (c) The entities included in the joint notice must provide the notice to individuals in accordance with the applicable requirements of this section. Provision of the joint notice to an individual by any one of the entities included in the joint notice will satisfy the provision requirement of this section with respect to all others by the joint notice. *[Reference: 45 C.F.R. § 164.520(d)]*
2.2.9 Documentation	An entity must document compliance with the notice requirements, by retaining copies of the notices issued by the entity and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment. *[Reference: 45 C.F.R. § 164.520(e)]*

2.3 REQUEST RESTRICTIONS	
An entity must permit an individual to request that the entity restrict uses or disclosures of their individual health information:	
2.3.1 Request for Restriction	For uses and disclosures related to treatment, payment, or health care operations. *[Reference: 45 C.F.R. § 164.522 (a)(i)]*
	For uses related to involvement in the individual's care and notification purposes *[Reference: 45 C.F.R. § 164.522 (a)(i)]*
2.3.2 Required Restrictions	An entity shall comply with a requested restriction if: (a) Except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and (b) The individual health information pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full. *[Reference: American Reinvestment and Recovery Act of 2009, Health Information Technology for Economic and Clinical Health Act, Section 13405]*
2.3.3 Option to Agree to Restrictions	The entity is not required to agree to the restriction unless the individual has paid out-of-pocket for their medical item or service. *See section 2.3.2.* *[Reference: 45 C.F.R. § 164.522(a)(1)(ii)]*
2.3.4 Agreeing to a Restriction	An entity that agrees to or is required to agree to a restriction under this section may not use or disclose individual health information in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted individual health information is needed to provide the emergency treatment, the entity may use the restricted individual health information, or may disclose such information to a health care provider, to provide such treatment to the individual. [*Reference: 45 C.F.R. § 164.522 (a)(1)(iii)]*
2.3.5 Exceptions to Restrictions – Involvement of Others in Individual's Care or Payment	An entity may disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the individual health information directly relevant to such person's involvement with the individual's care or payment related to the individual's health care. An entity may use or disclose individual health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or

	death. If the individual is present for, or otherwise available prior to, a use or disclosure permitted by this section and has the capacity to make health care decisions, the entity may use or disclose the individual health information if it: (a) Obtains the individual's agreement; (b) Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or (c) Reasonably infers from the circumstances, based the exercise of professional judgment that the individual does not object to the disclosure. If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the individual health information that is directly relevant to the person's involvement with the individual's health care. An entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of individual health information. [*Reference: 45 C.F.R. § 164.522(a)(1)(i)(B), 45 C.F.R. § 164.510(b)]*
2.3.6 Emergency Treatment	If an entity discloses restricted individual health information to a health care provider for emergency treatment, the entity must request that such health care provider not further use or disclose the information. [*Reference: 45 C.F.R. § 164.522 (a)(1)(iv)]*
2.3.7 Invalid Restriction	A restriction agreed to by an entity under this section, is not effective to prevent uses or disclosures permitted or required when: (a) Required by the Secretary of Health and Human Services, Department of Public Health, or California of Office of Health Information Integrity to investigate. *[see Sections 3.1.4.2 & 3.1.4.3]* ~~(b) Used for facility directory [see section X]~~ (c) The use or disclosure does not require authorization or opportunity to agree or object as permitted by these guidelines. *(See Section 3)* (d) The use or disclosure is otherwise permitted by these guidelines. *(See Section 3)* [*Reference: 45 C.F.R. § 164.522 (a)(1)]*
2.3.8 Terminating or Modifying a Restriction	An entity may terminate its agreement to a restriction, if: (a) The individual agrees to or requests the termination in writing; (b) The individual orally agrees to the termination and the oral agreement is

	documented; or (c) The entity informs the individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to individual health information created or received after it has so informed the individual. [*Reference: 45 C.F.R. § 164.522 (a)(2)]*

2.4 ACCESS TO INFORMATION BY THE INDIVIDUAL AND OTHERS	
An individual or his/her personal representative *(see section 1.4.2)* has the right to access his/her designated record set that is in the custody or under the control of an entity. An entity shall establish a process to receive all requests for access to individual health information.[1]	
2.4.1 Prohibition on Withholding Records	An entity shall not withhold the individual health information requested by an individual because of an unpaid bill for health care services. *[Reference: California Health and Safety Code § 123110(j)]*
2.4.2 Verification of Identity	Notwithstanding any other law, an entity may require reasonable verification of identity prior to permitting access to individual health information, provided this requirement is not oppressively used or discriminatory to frustrate or delay access. *[Reference: California Health and Safety Code § 123110(g)]*
2.4.3 Records Available to Access	An individual or his/her personal representative *(see Section 1.0)* has the right to access individual health information in his/her designated record set collected, created, requested, received or maintained by either an entity or its business associate to make decisions about an individual, for as long as the individual health information is maintained.
2.4.4 Records Exempt from Access	An individual or his/her personal representative *(see Section 1.0)* has the right to access his/her individual health information that is in the custody or under the control of an entity. An entity shall establish a process to receive all requests for access to individual health information, except for.[2]
2.4.4.1 DATA IN TRANSMISSION	Data that is in transmission.
2.4.4.2 PSYCHOTHERAPY NOTES	Psychotherapy notes are not available for access by an individual when a health care provider determines in the exercise of professional judgment, that there is a substantial risk of significant adverse or detrimental consequences to an individual, subject to several conditions. *[Reference: 45 C.F.R. § 164.501, Health and Safety Code § 123115(b), 45 C.F.R. § 164.524(a)(1) & Federal Register, Volume 65, Number 250,*

[1] *[References: California Privacy and Security Advisory Board Principle 3 – Individual Participation; 45 C.F.R. § 164.524 (a)-(e) Access to Protected Health Information; CMIA CA Civil Code Section 56.07; Health and Safety Code Section 123110(b), HITECH Section 13405(e), Canada Personal Health Information Protection Act, 2004, Part V Access to Records of Personal Health Information and Correction, NY Privacy and Security Policies and Procedures for RHIOs and their Participants in New York State]*

[2] *[References: California Privacy and Security Advisory Board Principle 3 – Individual Participation; 45 C.F.R. § 164.524 (a)-(e) Access to Protected Health Information; CMIA CA Civil Code Section 56.07; Health and Safety Code Section 123110(b), HITECH Section 13405(e), Canada Personal Health Information Protection Act, 2004, Part V Access to Records of Personal Health Information and Correction, NY Privacy and Security Policies and Procedures for RHIOs and their Participants in New York State]*

	Thursday, December 28, 200, Rules and Regulations, page 82733]
2.4.4.3 SAFETY	Notwithstanding any other law, individuals shall have access to mental health records unless a licensed health care provider, in the exercise of professional judgment determines that the access requested is reasonably likely to endanger the life or physical safety of the individual. *[Reference: 45 C.F.R. § 164.501, 45 C.F.R. § 164.524(a), & Health and Safety Code § 123115(b)]*
2.4.4.4 JUDICIAL OR ADMINISTRATIVE PROCEEDING	Information compiled in anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. *[Reference: 45 C.F.R. § 164.524(a)(1)(ii)]*
2.4.4.5 CLINICAL LABORATORIES	Information held by clinical laboratories under the jurisdiction of the Clinical Laboratory Improvements Amendments (CLIA). Only persons licensed under the provisions of state law relating to the healing arts or their representatives may receive clinical laboratory test records and reports. However, once the health care provider has disclosed the laboratory results to the individual, he/she may access such results. *(See section 2.4.5.3 & 2.4.5.4 for additional restrictions on provision of laboratory results electronically.)* *[Reference: 42 U.S.C. 263a, 45 C.F.R. § 164.524(a)(1)(iii)(A) & Business and Professions Code § 1288]*
2.4.4.6 EXEMPT FROM CLIA	Information maintained by entities exempt from the CLIA, which include. (a) Any facility or component of a facility that only performs testing for forensic purposes; (b) Research laboratories that test human specimens but do not report patient specific results for diagnosis, prevention or treatment of any disease or impairment of, or the assessment of the health of individual patients; or (c) Laboratories certified by the Substance Abuse and Mental Health Services Administration (SAMSHA), in which drug testing is performed which meets SAMSHA guidelines and regulations. However, all other testing conducted by a SAMHSA-certified laboratory is subject to CLIA. *[Reference: 45 C.F.R. § 164.524(a)(1)(iii)(B) & 42 C.F.R. § 493.3(a)(2)]*
2.4.4.7 ALCOHOL AND DRUG ABUSE RECORDS	Alcohol and drug abuse records, to the extent that access is prohibited by federal law or regulations. *(See Public Law 92-255, Public Law 91-616, or 43 C.F.R. Part 2)* *[Reference: Health and Safety Code § 123125]*
2.4.4.8 COMMUNICABLE DISEASE RECORDS	The individual health information of communicable disease carriers to the extent that access is limited by State or federal law. *[Reference: Health and Safety Code § 123125]*

2.4.4.9 SAFETY OF CORRECTIONAL OFFICERS	An entity that is a correctional institution or a covered health care provider acting under the direction of the correctional institution may deny, in whole or in part, an inmate's request to obtain a copy of individual health information, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate. *[Reference: 45 C.F.R. § 164.524(a)(2)(ii)]*
2.4.4.10 ONGOING RESEARCH	An individual's access to his/her health information created or obtained by an entity in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the entity has informed the individual that the right of access will be reinstated upon completion of the research. *[Reference: 45 C.F.R. § 164.524(a)(2)(iii)]*
2.4.4.11 PRIVACY ACT	An individual's access to his/her health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law. *[Reference: 45 C.F.R. § 164.524(a)(2)(iv)]*
2.4.4.12 CONFIDENTIALLY ACQUIRED INFORMATION	An individual's access may be denied if the individual health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information. *[Reference: 45 C.F.R. § 164.524(a)(2)(v)]*
2.4.4.13 REFERS TO ANOTHER PERSON	The individual health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person. *[Reference: 45 C.F.R. § 164.524(a)(3)(ii)]*
2.4.5 Minors	An entity shall allow a minor to access his/her individual health information in accordance with Sections 1.3.2 and 1.3.3. An entity shall not provide access to the individual health information of a minor when the entity determines that access to the minor's health information would have a detrimental effect on: (a) The health care provider's professional relationship with the minor patient, (b) The minor's physical safety or

	(c) The minor's psychological well-being. *[Reference: Health and Safety Code § 123115(a)(1)]*
2.4.6 Providing Access	When an entity provides an individual with access, in whole or in part, to individual health information, the entity shall comply with the following requirements. (a) The entity shall provide the access requested by individuals, including inspection or obtaining a copy, or both, of the individual health information about them. If the same individual health information that is the subject of a request for access is maintained in more than one location, the entity need only produce the individual health information once in response to a request for access. (b) The entity shall provide the individual with access to the individual health information in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the entity and the individual. *[Reference: 45 C.F.R. §§ 164.524I(1) & I(2)(i)]*
2.4.6.1 ELECTRONIC ACCESS	In the case that an entity uses or maintains an electronic health record (EHR) with respect to individual health information of an individual, the individual shall have a right to obtain from such entity a copy of such information in an electronic format and, if the individual chooses, to direct the entity to securely transmit such copy directly to an entity or person designated by the individual, provided that any such choice is clear, conspicuous, and specific. *[Reference: American Reinvestment and Recovery Act of 2009, Health Information Technology for Economic and Clinical Health Act, Section 13405 (e)]*
2.4.6.2 READABILITY	When providing access to individual health information an entity may provide in a reasonable fashion the explanation of term, code, or abbreviations used in the information. *[Reference: Canada Personal Health Information Protection Act, 2004]*
2.4.6.3 SPECIAL PROVISIONS FOR ACCESS TO LABORATORY TEST RESULTS	An entity, at whose request a clinical laboratory test be performed, shall provide the results of the test to the individual who is subject of the test if requested in writing or orally by the individual within a reasonable time period after the test results are received by the licensed health care professional who requested the test. (a) An entity may not charge the individual a fee for provision of laboratory test results when the request is provided in a manner other than electronic. (b) The results shall be conveyed in plain language.

	[Reference: California Health and Safety Code 123148(a)]
2.4.6.3.1 Test Results	The results may be conveyed in electronic form if requested by the individual and if deemed appropriate by the licensed health care professional who requested the test, and: (a) The individual provides an authorization permitting the provision of his/her laboratory results by the Internet or other electronic manner. The authorization may be revoked by the individual at any time. (b) Electronic access shall be restricted by the use of a secure personal identification number. (c) The licensed health care professional reviews the results. The licensed health care professional's determination that the provision of laboratory results electronically is appropriate may be revoked at any time. (d) The results are delivered to the individual within a reasonable time. (e) The test results do not contain individual health information concerning: (i) HIV antibody test, (ii) Presence of antigens indicating a hepatitis infection, (iii) Abusing the use of drugs, (iv) Routinely processed tissues, including skin biopsies, pap smear tests, products of conception, and bone marrow aspirations for morphological evaluation, if they reveal a malignancy. *[Reference: California Health and Safety Code Sections 123148(b)(1), (e), (f), & (j)]*
2.4.6.3.2 Direct Communication	Nothing in section 2.4.6.3.1 shall prohibit the direct communication by Internet posting or use of other electronic means to convey clinical laboratory test results by: (a) A treating health care professional who ordered the test for the individual or (b) A health care professional acting on behalf of, or with the authorization of, the treating health care professional who ordered the test. *[Reference: California Health and Safety Code Section 123148(b)(2)]*
2.4.6.3.3 Fees	An entity shall inform the individual of any fees that may be assessed directly to the individual or insurer for the Internet posting of the laboratory test results. *[Reference: California Health and Safety Code Section 123148(c)]*
2.4.6.3.4 Explanation	An individual may contact the licensed health care professional for a more detailed explanation of the laboratory test results when delivered.

	[Reference: California Health and Safety Code Section 123148(c)]
2.4.6.3.5 Record	Laboratory test results reported to the individual electronically shall be recorded in the individual's designated record set. *[Reference: California Health and Safety Code Section 123148(e)]*
2.4.6.3.6 Commercial Use	Laboratory test results and individual health information that has been provided under this section shall not be used for any commercial purposes without a valid authorization by the patient. Any third party that laboratory test results are disclosed shall be subject to these guidelines. *[Reference: California Health and Safety Code Sections 123148(g) & (h)]*
2.4.6 Summaries	An entity may provide the individual with a summary of the individual health information requested, in lieu of providing access to the individual health information or may provide an explanation of the individual health information to which access has been provided, if: (a) The individual agrees in advance to such a summary or explanation; and (b) The individual agrees in advance to the fees imposed, if any, by the covered entity for such summary or explanation. *[45 C.F.R. §§ 160.201 & 164.524(c)(2)(ii)]*
2.4.8 Request and Timely Action	An entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement. *[Reference: 45 .F.R. § 164.524(b)(1) & California Health and Safety Code § 123110(a)]*
2.4.8.1 TYPES OF REQUESTS FOR ACCESS	Nothing may prevent an entity from granting an individual access to his/her individual health information to which the individual has a right of access if the individual makes an oral request for access or does not make any request for access. [*Reference: 45 C.F.R § 164.524(b)(1) & Canada Personal Health Information Protection Act, 2004]*
2.4.8.2 ACTIONS ON REQUESTS	An entity shall act on a request for access as follows. (a) If an individual requests to access their records, an entity shall permit this access during business hours within five (5) working days after receipt of a request. *[Reference: Health and Safety Code §123110(a)]* (b) An individual or a personal representative shall be entitled to copies of all or any portion of the individual records that he/she has a right to access, upon presenting a request to the entity specifying the records to be copied. The entity shall ensure that the copies are transmitted within 15 days after receiving the written request.

	[Reference: Health and Safety Code §123110(b)] (c) If the entity grants the request, in whole or in part, it shall inform the individual of the acceptance of the request and provide the access requested. *[Reference: 45 C.F.R. § 164.524(b)(2)(i)(A)]* (d) If the entity denies the request, in whole or in part, it shall provide the individual with a written denial. *[Reference: 45 C.F.R. § 164.524(b)(2)(i)(B)]]* (e) The entity shall provide the access as requested by the individual including arranging with the individual for a convenient time and place to or obtain a copy of the individual health information, or mailing the copy of the individual health information at the individual's request. *[Reference: 45 C.F.R. § 164.524(c)(3)]*
2.4.9 Expedited Access	An entity may provide expedited access to individual health information within the time period requested, if the individual provides the entity with evidence satisfactory to the entity that access is urgent. *[Reference: Canada Personal Health Information Protection Act, 2004]*
2.4.10 Fees	An entity may charge the cost of copying, including the cost of supplies for and labor of copying as long as the amount does not exceed twenty-five ($.25) a page for copies of an individual's health information. An entity may charge fifty cents ($.50) per page for records that are copied from microfilm. If the individual agrees to a summary or explanation of such information, the entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of preparing an explanation or summary of the individual health information, if agreed to by the individual. *[Reference: 45 C.F.R. §§ 164.524(b)(4) and (c)(4) & Health and Safety Code. § 123110 (b)]*
2.4.11 Electronic Copies	If the entity acquires an electronic health record system and is providing electronic access to records then any fee that the entity may impose for providing such individual with a copy of such information (or a summary or explanation of such information) if such copy (or summary or explanation) is in an electronic form shall not be greater than the entity's labor costs in responding to the request for the copy (or summary or explanation). [*Reference: American Reinvestment and Recovery Act of 2009, Health Information Technology for Economic and Clinical Health Act, Section 13405(e)]*

2.4.12 Public Benefit Program Purpose	Any individual or their representative shall be entitled to a copy, at no charge, of the relevant portion of the individual's health information, upon presenting to the provider a written request, and proof that the records are needed to support an appeal regarding eligibility for a public benefit program. (a) Although an individual shall not be limited to a single request, the individual or their representative shall be entitled to no more than one copy of any relevant portion of his or her record free of charge. (b) This shall not apply to any individual who is represented by a private attorney who is paying for the costs related to the individual's appeal, pending the outcome of that appeal. (c) The health care provider shall ensure that the copies are transmitted within 30 days after receiving the written request. If the individual's appeal regarding eligibility for a public benefit program is successful, the hospital or other health care provider may bill the individual for the copies of the individual health information previously provided free of charge. *[Reference: Health and Safety Code § 123110(d)&(f)]*
2.4.13 Records Not Found	If the records are not found or do not exist the entity shall provide written notice to the individual requesting the individual health information. If the entity cannot identify or locate the individual health information requested because there is not sufficient detail to do so, the entity may offer assistance to the person requesting access in reformulating the request. *[Reference: Canada Personal Health Information Protection Act, 2004]*
2.4.14 Unreviewable Denials of Access	Entities may deny, in whole or in part, access by an individual to his/her individual health information when the information is: (a) Excepted from the right of access *[see list above in Section 2.3.3]* (b) Related to an inmate's request to obtain a copy of individual health information, from an entity that is a correctional institution or a health care provider acting under the direction of the correctional institution, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate. *[Reference: 45 C.F.R. § 164.524(a)(2)(ii)]* (c) Created or obtained by a health care provider in the course of research that includes treatment. Access may be temporarily suspended for as long as the research is in progress, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the entity has informed the individual that the right of access will be reinstated upon completion of the research.

	[Reference: 45 C.F.R. § 164.524(a)(2)(iii)] (d) An individual's access to individual health information that is contained in records that are subject to the Privacy Act, 5 U.S.C. § 552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law. *[Reference: 45 C.F.R. § 164.524(a)(2)(iv)]* (e) An individual's access may be denied if the individual health information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information. *[Reference: 45 C.F.R. § 164.524(a)(2)(v)]*
2.4.15 Reviewable Denials of Access	An individual has the right to request a review by a licensed health care professional identified by the entity of denials of access that are conditional. The following are conditional access rights and an entity may deny access when: (a) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person; *[Reference: 45 C.F.R. § 164.524(a)(3)(i)]* (b) The individual health information makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or *[Reference: 45 C.F.R. § 164.524(a)(3)(ii)]* (c) The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person. *[Reference: 45 C.F.R. § 164.524(a)(3)(iii)]*
2.4.15.1 REQUIRED ACTIONS FOR REVIEWABLE DENIALS OF ACCESS	In the exercise of any of the above reviewable denial actions, a licensed health care professional is required to mask any individual health information that is subject to conditional access by the individual. System or systems permitting access to those records shall mask such individual health information to prevent access to the individual health information by the individual. Only a licensed health care professional can determine when the individual health information will be accessible. *[Reference: 45 C.F.R. § 164.524(d)]*
2.4.15.2 SPECIAL PROVISIONS FOR	When a health care provider determines there is a substantial risk of

DENIAL TO PSYCHOTHERAPY NOTES	significant adverse or detrimental consequences to an individual in seeing or receiving a copy of psychotherapy notes requested by the individual, the provider may decline to permit inspection or provide copies of the notes to the individual, subject to the following conditions: (a) The health care provider shall make a written record, to be included with the psychotherapy notes, noting the date of the request and explaining the health care provider's reason for refusing to permit inspection or provide copies of the notes, including a description of the specific adverse or detrimental consequences to the individual that the provider anticipates would occur if inspection or copying were permitted. (b) The health care provider shall permit inspection by, or provide copies of the psychotherapy notes to, a licensed physician and surgeon, licensed psychologist, licensed marriage and family therapist, or licensed clinical social worker, designated by request of the individual. The licensed physician and surgeon, licensed psychologist, licensed marriage and family therapist, licensed clinical social worker, or marriage and family therapist registered intern to whom the notes are provided for inspection or copying shall not permit inspection or copying by the individual. (c) The health care provider shall inform the individual of the provider's refusal to permit him or her to inspect or obtain copies of the requested notes, and inform the individual of the right to require the provider to permit inspection by, or provide copies to, a licensed physician and surgeon, licensed psychologist, licensed marriage and family therapist, or licensed clinical social worker, designated by written authorization of the individual. (d) The health care provider shall indicate in the psychotherapy notes of the individual whether the request would have a detrimental effect on the provider's professional relationship with the individual or the physical safety or psychological well-being. *[Reference: 45 C.F.R. §§ 160.201-164-205, Health and Safety Code § 123115(b)]*
2.4.16 Entity Duties for Denial of Access	When an entity denies access, in whole or in part, to individual health information, the entity shall comply with the following requirements. (a) An entity shall, to the extent possible, give the individual access to any other individual health information requested, after excluding the individual health information as to which the entity has a ground to deny access. (b) An entity shall provide a timely, written denial to the individual. The denial shall be in plain language and contain: (i) The basis for the denial; (ii) If applicable, a statement of the individual's review rights, including

	a description of how the individual may exercise such review rights; and (iii) A description of how the individual may complain to the entity, to the Secretary of the U.S. Department of Health and Human Services. *(See section 4.6*) The description shall include the name, or title, and telephone number of the contact person or office. (iv) If the entity was not the licensed health care professional who originally denied access or masked the individual health information, the entity shall inform the individual of the responsible party. *[Reference: 45 C.F.R. § 164.524(d)(2)]*
2.4.17 Individual Request for Review of Denial	If an individual has requested a review of a denial pursuant to section 2.4.15, the entity shall designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The entity shall promptly refer a request for review to such designated reviewing official. The designated reviewing official shall determine, within a reasonable period of time, whether or not to deny the access. The entity shall promptly provide written notice to the individual of the determination of the designated reviewing official and take other action to carry out the designated reviewing official's determination. *[Reference: 45 C.F.R. § 164.524(d)(4)]*
2.4.18 Entity's Responsibility to Inform	If an entity does not maintain the individual health information that is the subject of the individual's request for access, and the entity knows where the requested information is maintained, the entity shall inform the individual where to direct the request for access. *[Reference: 45 C.F.R. § 164.524(d)(3)]*

2.5 REQUEST ALTERNATIVE COMMUNICATIONS	
2.5.1Requests to Entities	An entity, other than a health plan, shall permit individuals to request and shall accommodate reasonable requests by individuals to receive communications of individual health information from the entity by alternative means or at alternative locations. [*Reference: 45 C.F.R. § 164.522 (b)(1)]*
2.5.2 Requests to Health Plans	A health plan shall permit individuals to request and shall accommodate reasonable requests by individuals to receive communications of individual health information from the health plan by alternative means or at alternative locations, if the individual clearly states that the disclosure of all or part of that information could endanger the individual. [*Reference: 45 C.F.R. § 164.522 (b)(1)(ii)]*
2.5.3 Requirements of the Individual	An entity may require the individual to make a request for a confidential communication in writing. An entity may condition the provision of a reasonable accommodation when appropriate, on information as to: (a) How payment, if any, will be handled; and (b) Specification of an alternative address or other method of contact. An entity, other than a health plan, may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis. However, a health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual. [*Reference: 45 C.F.R. § 164.522 (b)(2)(i)-(iv)]*
2.5.4 Electronic Format	In the case that an entity uses or maintains an electronic health record with respect to individual health information, the individual shall have a right to obtain from such entity a copy of such information in an electronic format and, if the individual chooses, to direct the entity to securely transmit such copy directly to an entity or person designated by the individual, provided that any such choice is clear, conspicuous, and specific. [*Reference: American Reinvestment and Recovery Act of 2009, Health Information Technology for Economic and Clinical Health Act Section 13405(e)]*

2.6 AMENDMENTS	
An individual has the right to have an entity amend his/her individual health information or a record about the individual in a designated record set for as long as the individual health information is maintained by the entity.[3]	
2.6.1 Addendums	An individual has the right to submit to an entity an addendum to his/her designated record set. An entity shall accept and place into the designated record set an addendum limited to 250 words per alleged incomplete or incorrect item received from an individual. The designated record set shall clearly indicate in writing that the addendum is part of the record. An entity shall attach the addendum to the designated records set and include the addendum whenever a disclosure is made to any third party of the allegedly incomplete or incorrect individual health information. *[Reference: Health and Safety Code § 123111]*
2.6.2 Amendments	An entity shall permit an individual to request that the entity make an amendment to his/her health information maintained by the entity. The entity may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements. [*Reference: 45 C.F.R.§164.526(b)(1)]*
2.6.3 Timely Response to Request for Amendment	An entity shall act on the individual's request for an amendment no later than 60 days after receipt of such a request, as follows. (a) If the entity is unable to act on the amendment within the time required, the entity may extend the time for such action by no more than 30 days, provided that: (b) The entity provides the individual with a written statement of the reasons for the delay and the date by which the entity will complete its action on the request; and (c) The entity may have only one such extension of time for action on a request for an amendment. [*Reference: 45 C.F.R.§164.526(b(2))]*
2.6.4 Informing about Amendment	An entity shall timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the entity notify the relevant persons with which the amendment needs to be shared. An entity shall make reasonable efforts to inform and provide the amendment within a reasonable time to:

[3] *[References: California Privacy and Security Advisory Board Principle 3 – Individual Participation; 45 C.F.R.§164.526 (a)-(f) Right to Amend; Health and Safety Code Section 123111(a)-(d), & Canada Personal Health Information Protection Act, 2004, Part V Access to Records of Personal Health Information and Correction]*

	(a) Persons identified by the individual as having received individual health information about the individual and needing the amendment; (b) Persons or entities that the entity's records indicate have had access to or that the amended individual health information has been disclosed, and (c) Persons, including business associates, that the entity knows have the individual health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual. [*Reference: Canada Personal Health Information Protection Act, 2004 & 45 C.F.R.§164.526(c)(2) & (c)(3)(i) & (c)(3)(ii)]*
2.6.5 Denial of Amendment	An entity may deny an individual's request for amendment, if it determines that the individual health information or record that is the subject of the request: (a) Was not created by the entity, unless the individual provides a reasonable basis to believe that the originator of the individual health information is no longer available to act on the requested amendment; (b) Is not part of the entity's records; (c) Would not be available for inspection by the Secretary of Health and Human Service, or (d) Is accurate and complete. An entity may not deny an individual's request to have an addendum added to his/her designated record set. [*Reference: 45 C.F.R.§164.526(a)(2)]*
2.6.6 Request Denied	An entity shall provide the individual with a timely, written denial of the requested amendment. The denial shall use plain language and contain: (a) The basis for the denial; (b) The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement; (c) A statement that, if the individual does not submit a statement of disagreement, the individual may request that the entity provide the individual's request for amendment and the denial with any future disclosures of the individual health information that is the subject of the amendment; and (d) A description of how the individual may complain to the entity pursuant to the complaint process *[see section 4.6]* or to the Secretary of the U.S. Department of Health and Human Services. The description shall include the name, or title, and telephone number of the contact person or office. [*Reference: 45 C.F.R.§164.526(d)(1)(i)-(iv)]*

2.6.7 Statement of Disagreement	An entity shall permit the individual to submit to the entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The receipt of information in a patient's addendum *(see Section 2.6.1)* which contains defamatory or otherwise unlawful language, and the inclusion of this information in the patient's records, shall not, in and of itself, subject the health care provider to liability in any civil, criminal, administrative, or other proceeding. *[Reference: 45 C.F.R.§164.526(d)(2) & Health and Safety Code § 123111]*
2.6.8 Rebuttal	An entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the entity shall provide a copy to the individual who submitted the statement of disagreement. *[Reference: 45 C.F.R.§164.526(d)(3)]*
2.6.9 Record Linkage for Denials	An entity shall, as appropriate, identify the individual health information that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the entity's denial of the request, the individual's statement of disagreement, if any, and the entity's rebuttal, if any, to the record. *[Reference: 45 C.F.R.§164.526(d)(4)]*
2.6.10 Future Disclosures	If a statement of disagreement has been submitted by the individual, the entity shall include the material appended, at the election of the entity, an accurate summary of any such information, with any subsequent disclosure of the individual health information to which the disagreement relates. If the individual has not submitted a written statement of disagreement, the entity shall include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the individual health information only if the individual has requested such action. When a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included with the disclosure, the entity may separately transmit the material required, as applicable, to the recipient of the standard transaction. [*Reference: 45 C.F.R.§164.526(d)(5)(i)-(iii)]*
2.6.11 Actions on Notice of Amendment	An entity that is informed by another entity of an amendment to an individual's individual health information, in accordance with this section, shall amend the individual health information in its records. *[Reference: 45 C.F.R.§164.526(e)]*

2.7 ACCOUNTING OF DISCLOSURES	
An individual has the right to receive an accounting of disclosures in these circumstances.	
2.7.1 Who May Request an Accounting of Disclosures	An individual may request an accounting of disclosures of their individual health information made by the entity. *[Reference: 45 C.F.R. § 164.528(a)(1)]*
2.7.2 Accounting for Entities without an EHR	An entity that has not acquired an electronic health record, shall provide an accounting of the disclosures in the six years prior to the request of: (a) Disclosures to public health authorities, (b) Disclosures that result from a requirement from another federal or State law or regulation, (c) Disclosures to any government entity, unless otherwise exempted, (d) Disclosures to all law enforcement, unless otherwise exempted, (e) Disclosures to insurers for claims investigations, (f) Disclosures concerning abuse, (g) Disclosures for research, or (h) Disclosures to health oversight agencies. However, an entity is not required to account for: (a) Disclosures to carry out treatment, payment, health care operations, (b) Disclosures to individuals of health information about themselves, (c) Incidental disclosures where the disclosure was otherwise permitted or required by law, (d) Disclosures pursuant to a valid authorization, (e) For the facility's directory or to persons involved in the individual's care or other notification purposes where the individual had an opportunity to agree or object to the disclosure, (f) Disclosures for national security or intelligence purposes for specified activities, (g) Disclosures to correctional institutions or law enforcement custodial situations for specified activities, (h) Disclosures that are made as part of a limited data set for research, health care operations or public health, or (i) Disclosures of de-identified data. *[Reference: 45 C.F.R. § 164.528(a)(1)(i)-(ix)]*
2.7.2.1 ACCOUNTING REQUIRED - EHR	In addition, an entity that has an electronic health record is required to account for disclosures to carry out treatment, payment, health care

	operations. *(See Section 2.7.4 below for implementation timeline.)* *[Reference: American Reinvestment and Recovery Act of 2009, Health Information Technology for Economic and Clinical Health Act Section 13405(c)]*
2.7.3 Timeline for Treatment, Payment and Health Care Operations Accountings	For an entity who has acquired an electronic health record after January 1, 2009, they shall account for the above disclosures, as well as all other disclosures for treatment, payment, or health care operations in the past three (3) years. (a) For an entity that has acquired an electronic health record on or before January 1, 2009, they shall comply by January 1, 2014. (b) For an entity that has acquired an electronic health record after January 1, 2009, they shall comply by the later date of January 1, 2011, or the date that it acquires an EHR. *[Reference: American Reinvestment and Recovery Act of 2009, Health Information Technology for Economic and Clinical Health Act Section 13405(c)]*
2.7.4 Special Considerations - EHR	For an entity who has acquired an electronic health record, they may provide: *(a)* An accounting as stated above of disclosures that are made by the entity and their business associate, or *(b)* An accounting of disclosures made by the entity and a list of all business associates who disclose individual health information on behalf of the entity, including contact information for such associates (such as mailing address, phone, and email address). A business associate included on the list shall provide an accounting of disclosures made by the business associate upon a request made by an individual directly to the business associate for such an accounting. *[Reference: American Reinvestment and Recovery Act of 2009, Health Information Technology for Economic and Clinical Health Act Section 13405(c)]*
2.7.5 Suspension of Accounting	An entity shall temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by such agency or official, if such agency or official provides the entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required. If the agency or official statement is made orally, the entity shall: (a) Document the statement, including the identity of the agency or official making the statement

	(b) Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and (c) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time *[Reference: 45 C.F.R. § 164.528(a)(2)(i)]*
2.7.6 Accounting of Disclosures Log	An individual may request an accounting of disclosures for a period of time less than six years from the date of the request. The entity shall include the following disclosure information in the accounting: (a) The date of the disclosure, (b) The name of the entity or person who received the individual health information, (c) The address of the entity or person, if known, (d) A brief description of the individual health information disclosed, and (e) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, (f) In lieu of such a statement, a copy of a written request for a disclosure.
2.7.7 Response to Request for Accounting of Disclosures	In response to a request from an individual for an accounting, an entity shall elect to provide either an: (a) Accounting for disclosures of individual health information that are made by an entity and by a business associate acting on behalf of an entity, or (b) An accounting of disclosures that are made by such entity and provide a list of all business associates acting on behalf of the entity including contact information for such associates (such as mailing address, telephone number, and email address). A business associate included on a list shall provide an accounting of disclosures for an entity made by the business associate upon a request made by an individual directly to the business associate for such an accounting. *[Reference: 45 C.F.R. § 164.528(b)(1) & (b)(2)(i)-(iv); California Civil Code § 1798.25; and the American Reinvestment and Recovery Act of 2009, Health Information Technology for Economic and Clinical Health Act, Section 13405(c)]*
2.7.8 Multiple Disclosures	If, during the period by the accounting, an entity has made multiple disclosures of individual health information to the same person or entity for a single purpose, the accounting may provide: (a) The information required above, (b) The frequency, periodicity, or number of disclosures made during the

	accounting period, and (c) The date of the last such disclosure during the accounting period. *[Reference: 45 C.F.R. § 164.528(b)(3)]*
2.7.9 Research	If during the period by the accounting, an entity has made disclosures of individual health information for a particular research purpose for 50 or more individuals, the accounting may, with respect to such disclosure for which the individual health information about the individual may have been included, provide: (a) The name of the protocol or other research activity; (b) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records; (c) A brief description of the type of individual health information that was disclosed; (d) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period; (e) The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and (f) A statement that the individual health information of the individual may or may not have been disclosed for a particular protocol or other research activity. If an entity provides an accounting for research disclosures and if it is reasonably likely that the individual health information of the individual was disclosed for such research protocol or activity, the entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher. *[Reference: 45 C.F.R. § 164.528(b)(4)(i)]*
2.7.10 Timing	An entity shall act on the individual's request for an accounting no later than 60 days after receipt of the request, as follows: (a) An entity shall provide the individual with the accounting requested, or (b) If an entity is unable to provide the accounting within 60 days, the entity may extend the time to provide the accounting by no more than 30 days, provided that: (i) Within the 60 days after receipt of the request, the entity provides the individual with a written statement of the reasons for the delay and the date by which the accounting will be provided, and (ii) The entity may have only one such extension. *[Reference: 45 C.F.R. § 164.526(c)(1)(i)&(ii) & American Reinvestment*

	and Recovery Act of 2009, Health Information Technology for Economic and Clinical Health Act, Section 13405(c)(1)]
2.7.11 Fees	An entity shall provide the first accounting to an individual in any 12-month period without charge. The entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the entity: (a) Informs the individual in advance of the fee, and (b) Provides the individual with an opportunity to withdraw, or (c) Modifies the request for a subsequent accounting to avoid or reduce the fee. *[Reference: 45 C.F.R. § 164.528(c)(2)]*

3.1 GENERAL USE AND DISCLOSURE	
3.1.1 Applicability	The following guidelines shall apply to all individual health information maintained or transmitted by an entity, except as otherwise specified. The request, use, and disclosure of individual health information shall be limited to protect the privacy of the individual. An entity may not electronically exchange individual health information with another entity unless: *[California Privacy and Security Advisory Board Scope Statement]*
3.1.1.1 HIECONSENT	The entity has informed the individual of their HIEconsent options. *[See Section 2.1]*
3.1.1.2 LAW	The request, use, or disclosure is required or permitted by law or these guidelines. *[Reference: California Privacy and Security Advisory Board Mission Statement, Vision, Principles 4, 5, & 6; 45 C.F.R. §§ 164.502(a)(iv) & (vi), California Civil Code 56.10, 56.1007, 56.101, 56.102, 56.11]*
3.1.2 Purpose Limit	An entity shall request, use, and disclose only the individual health information reasonably necessary to accomplish the purpose and as limited by the permitted uses and disclosures of individual health information reflected in these guidelines. *(See Section 3.0-3.4)* *[45 C.F.R. § 164.5514(d)(2), (3), & (4)]*
3.1.3.2 KNOWLEDGE	An entity shall inform individuals of the purpose for which his/her individual health information will be used and/or disclosed. Entities shall inform individuals of the following if their information will be exchanged electronically with any other entity outside of the collecting entity: (a) Entity's name receiving the information, and (b) The use or purpose for the disclosure of the information. *[See Section 2.0 Consent for more information about informing individuals.]* *[Reference: California Privacy and Security Advisory Board Principle 4, 5, & 6; HITECH Section 13405, 45 C.F.R. §§ 164.502(b)(1) & 164.514(d)]*
3.1.4 Required Disclosure	An entity is required to disclose individual health information to:
3.1.4.1 INDIVIDUAL	An individual, when the individual requests access as provided in Section 2.4. *[Reference: 45 C.F.R. § 164.502(a)(2), California Civil Code § 56.10(b)(7), California Health and Safety Code § 123110]*
3.1.4.2 SECRETARY OF DHHS	The Secretary of the U.S. Department of Health and Human Services when required to investigate or determine the entity's compliance with the Health Information Portability and Accountability Act, 45 C.F.R. Parts 160 and 164. *[Reference: California Civil Code § 56.10(b)(9) & 45 C.F.R. §*

	164.502(a)(2)(ii)]
3.1.4.3 GOVERNMENT AGENCIES	The Directors of the California Department of Public Health or the California Office of Health Information Integrity for purposes of compliance with these guidelines and State law. *[Reference: California Health and Safety Code § 1280.15 & 130200]]*
3.1.5 Minimum Necessary	An entity shall make reasonable efforts to limit requests, uses within the organization, and disclosures and exchanges outside the organization of individual health information to the minimum necessary to accomplish the purpose for which the information is being requested, used, or disclosed. *[Reference: 45 C.F.R. §§ 164.502(b) & 164.514(d)]*
3.1.5.1 AUTHORIZED USERS & CATEGORY	An entity shall limit requests, uses within the organization, and disclosures outside the organization of individual health information to those authorized users within their organization or authorized receivers outside the organization, specifically identified by their class or designated by the appropriate category of health information to be requested, used, or disclosed. *[Reference: 45 C.F.R. § 164.514(d)(2), (3) & (4); California Privacy and Security Advisory Board Principles 3, 4, & 5]*
3.1.5.2 ENTIRE MEDICAL RECORD	An entity may not request, use, or disclose an entire medical record or sets of records except when the entire medical record is specifically justified as the amount that is necessary to accomplish the purpose of the request, use, or disclosure. *[Reference: 45 C.F.R. § 164.514(d)(5); California Privacy and Security Advisory Board Principles 4, 5, & 6]*
3.1.5.3 NO MINIMUM NECESSARY EXCLUSIONS	Minimum necessary does not apply to: (a) Requests, uses, or disclosures by a health care provider for purposes of treatment as limited to the specific individual health information necessary for the health care provider to address the health care incident. (b) An individual's access to his/her individual health information. (c) Disclosures made pursuant to an authorization; however, the information to be disclosed shall be limited by the terms of the authorization. (d) Disclosures made to the Secretary of the U.S. Department of Health and Human Services or to the Directors of the California Department of Public Health or the California Office of Health Information Integrity. *[Reference: 45 C.F.R. § 164.505(a)(2) and (b)(3)(iv); California Civil Code § 56.36 and California Health and Safety Code § 1280.15.]* (e) Requests, uses, or disclosures required by law. *[Reference: 45 C.F.R. § 164.502(b)(2), NHIN Consumer Preference Profile]*
3.1.5.5 EXTERNAL REQUESTS	An entity may rely on the requested disclosure to be the minimum necessary for the stated purpose if the requestor represents that the request such, and

	(a) The information is requested by a member of the health information organization, (b) The information is requested by public officials who are permitted to have the information disclosed, (c) The information is requested by a professional who is a member of the requesting entity's workforce or its business associate for the purposes of providing professional services to the entity, or (d) Documentation or representations that comply with the guideline requirements to disclose information for research purposes have been provided by the person requesting the information. *[See Section 3.3.22 for more information about research requests.]* *[Reference: 45 C.F.R. § 164.514(d)(3)(iii); California Privacy and Security Advisory Board Principle 5]*
3.1.5.6 REQUESTS BY THE ENTITY	An entity must limit any requests for individual health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other entities. For requests that are made on recurring bases, the entity shall implement policies and procedures to accomplish the purpose for which the request is made. *[Reference: 45 C.F.R. §§ 164.502(b)(1) & 164.514(d)(4); California Privacy and Security Advisory Board Principle 4]*
3.1.5.7 USES	An entity participating in an HIE shall identify: (a) Those authorized users or classes of authorized users in its workforce who need access to individual health information to carry out their duties (b) The category or categories of individual health information to which access is required to carry out their duties and any conditions appropriate to such access. (c) An entity participating in an HIE shall limit the access of such authorized users or classes of authorized users to individual health information consistent with this requirement. Entities participating in an HIE shall share its access controls with the California Privacy and Security Advisory Board (California Privacy and Security Advisory Board), to enable the development of best practices to ensure access to necessary information as well as protect privacy from overly broad and unnecessary disclosures. *[References: 45 C.F.R. §§ 164.502(b) & 164.514(d)(2); California Privacy and Security Advisory Board Principle 5]*
3.1.5.8 DISCLOSURES	An entity shall implement policies and procedures to reasonably limit the disclosure of individual health information to the amount necessary to accomplish the purpose when such disclosures are made on recurring bases.

	For all other disclosures to which minimum necessary applies, an entity shall: (a) Develop criteria designed to limit the individual health information disclosed to the information necessary to accomplish the purpose for which disclosure is sought, and (b) Develop criteria designed to limit the disclosure to the: (i) Pertinent individual health information necessary to address the specified health care incident, and (ii) Appropriate person with a health care provider/patient relationship. An entity may implement the above criteria using security access controls and audit controls *(see Section 8.0).* *[Reference: 45 C.F.R. § 164.514(d)(3); California Privacy and Security Advisory Board Principle 5; NHIN Consumer Preference Profile]*
3.1.5.9 ENTIRE MEDICAL RECORD	An entity may not request, use, or disclose an entire medical record or sets of records except when the entire medical record is specifically justified as the amount that is necessary to accomplish the purpose of the request, use, or disclosure. *[Reference: 45 C.F.R. § 164.514(d)(5); California Privacy and Security Advisory Board Principles 4, 5, & 6]*
3.1.6 Authorization Use or disclosure	An entity is permitted to use or disclosure individual health information pursuant to and in compliance with a valid authorization. *[Reference: 45 C.F.R. §§ 164.502(a)(1)(iv), 164.508, California Civil Code § 56.10(a)]*
3.1.6.1 VALID AUTHORIZATION	A valid authorization is a document that contains the following: (a) A statement that remuneration is involved if the request, use, or disclosure being authorized involves direct or indirect remuneration for marketing to the entity from a third party, (b) The core elements required in section below, and (c) The statements required in section below. *[Reference: 45 C.F.R. § 164.508(b)(1)]*
3.1.6.1.1 Optional Elements	A valid authorization may contain elements or information in addition to the elements required by this section, provided that such additional elements or information are not inconsistent with the elements required by this section. *[Reference: 45 C.F.R § 164.508(b)(1)(ii)]*

3.1.6.1.2 Core Elements	(a) A description of the information to be used or limitations on the type of information to be disclosed that identifies the information in a specific and meaningful fashion. *[Reference: California Civil Code § 56.11(d)]* (b) The name or other specific identification of the person(s) or class of persons authorized to make and receive the requested use or disclosure. [*Reference:* California Civil Code § 56.11(f) (c) The name, function, or other specific identification of the person(s) or class of persons to whom the entity may make the requested use or disclosure. *[Reference: California Civil Code § 56.11(e)]* (d) A description of each purpose and limitation of the requested request, use, or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not or elects not to provide a statement of purpose. *[Reference: California Civil Code § 56.11(g)]* (e) A specific expiration date the authorization is no longer valid to disclose individual health information. *[Reference: 45 C.F.R. § 164.506(c)(1), California Civil Code § 56.11(h)]* (f) Is signed and dated by one of the following: (g) The individual. An individual who is a minor may only sign an authorization for the release of individual health information obtained in the course of furnishing services to which the minor could lawfully have consented. *(See section ___)* *[California Civil Code § 56.11(c)(1)]* (h) The personal representative of the patient, if the individual is a minor or incompetent. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided. *(See section 4.3___)* However, authorization may not be given for the disclosure of individual health information obtained in the course of furnishing health care services to which a minor could lawfully have consented. *(See section _____)* *[California Civil Code § 56.11(c)(2)]* (i) The beneficiary or personal representative of a deceased individual. *[California Civil Code § 56.11(c)(4)]* *[Reference: 45 C.F.R. § 164.506(c)(1)]*
3.1.6.1.3 Required Statements	In addition to the core elements, the authorization shall contain statements adequate to place the individual on notice of all of the following: (a) The individual's right to revoke the authorization in writing and either: (i) The exceptions to the right to revoke and a description of how the individual may revoke the authorization, or

	(ii) To the extent that the information directly above is included in the entity's Notice of Privacy Practices, a reference to such notice. (b) The ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization by stating either: (i) The entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations applies; or (ii) The consequences to the individual of a refusal to sign the authorization when the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization. (c) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by these guidelines. *[Reference: 45 C.F.R. § 164.508(c)]*
3.1.6.1.4 PLAIN LANGUAGE	The authorization must be written in plain language is in a typeface no smaller than 14 point type. The authorization may be handwritten by the individual who signs it. *[45 C.F.R. 164.506(c)(3) & California Civil Code § 56.11(a)]*
3.1.6.1.5 SEPARATE ACTION	The authorization is clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization. *[California Civil Code § 56.11(b)]*
3.1.6.1.6 COPY TO THE INDIVIDUAL	The entity shall provide the individual with a copy of the signed authorization if the entity seeks an authorization from the individual for a use or disclosure of individual health information. *[Reference: 45 C.F.R. § 164.508(c)(4)]*
3.1.6.2 Other – Authorizations Requirements	
3.1.6.2.1 REDISCLOSURE OF INFORMATION	An entity that receives individual health information pursuant to an authorization may not further disclose that individual health information except in accordance with a new authorization or as specifically required or permitted by law. *[Reference: California Civil Code § 56.13 & California Civil Code § 56.213]*
3.1.6.2.2 LIMITATIONS OF AUTHORIZATION	An entity that discloses individual health information pursuant to an authorization shall communicate to the person or entity to which it discloses the information any limitations in the authorization regarding the use of the information. No entity that has attempted in good faith to comply with this provision shall be liable for any unauthorized use of the individual health information by the person or entity to which the entity disclosed the information.

	[Reference: California Civil Code § 56.14]
3.1.6.2.3 DEFECTIVE AUTHORIZATIONS	An authorization is not valid, if the document submitted has any of the following defects: (a) The expiration date has passed or the expiration event is known by the covered entity to have occurred; (b) The authorization has not been filled out completely, with respect to an element described section 3.1.6.1.2, if applicable; (c) The authorization is known by the covered entity to have been revoked; (d) The authorization does not meet the criteria for a compound authorization or conditions the authorization inappropriately, if applicable; (e) Any material information in the authorization is known by the covered entity to be false. *[Reference: 45 C.F.R. § 164.508(b)(2)]*
3.1.6.2.4 PROHIBITION OF CONDITIONING OF AUTHORIZATIONS	An entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except: (a) A provider may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of individual health information for such research under this section; (b) A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if: (i) The authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and (ii) The authorization is not for a use or disclosure of psychotherapy notes; and (c) A covered entity may condition the provision of health care that is solely for the purpose of creating individual health information for disclosure to a third party on provision of an authorization for the disclosure of the individual health information to such third party. *[Reference: California Civil Code § 56.37 & 45 C.F.R. § 164.508(b)(4)]*
3.1.6.2.5 REVOCATIONS OF AUTHORIZATIONS	An individual may cancel or modify an authorization provided under this section at any time, provided the cancellation or modification shall be effective only after the entity actually receives written notice of the cancellation or modification. *[Reference: California Civil Code § 56.15]*
3.1.6.2.6 DOCUMENTATION OF	A covered entity must document and retain any signed authorization. *(See Section 4.4)* *[Reference: 45 C.F.R. § 164.508(b)(6)]*

AUTHORIZATIONS	
3.1.6.2.7 WAIVER	Any waiver by an individual to provide an authorization for disclosure of individual health information not permitted by law is contrary to public policy and shall not be enforceable. *[Reference: California Civil Code § 56.37]*
3.1.6.2.8 REBUTTABLE PRESUMPTIONS	The exchange by a health care provider of individual health information upon receipt of a request, in conformance with these guidelines, creates a rebuttable presumption that the release of individual health information was appropriate. A healthcare provider that discloses or uses individual health information in reliance upon the electronic affirmation of consent in the exchange and in conformance with these guidelines does not violate the Confidentiality of Medical Information Act *(Civil Code section 56 et seq.)*. *[Reference: California Civil Code § 56.36]*
3.1.7 De-Identified Information Use and Disclosure	An entity is permitted to use individual health information to create information that is not individually identifiable or disclose individual health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the entity. Health information that meets de-identification under these guidelines is not considered individually identifiable, i.e., de-identified. The requirements of these guidelines do not apply to de-identified information provided that: (a) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of individual health information. (b) If de-identified information is re-identified, an entity is permitted to use or disclose such re-identified information only as permitted or required by these guidelines. *[Reference: California Civil Code Section 56.05, Definition of Medical Information & 45 C.F.R. § 164.502(d)]*
3.1.7.1 DE-IDENTIFICATION OF INDIVIDUAL HEALTH INFORMATION	An entity may determine that health information is not individually identifiable health information only if: (a) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and (ii) Documents the methods and results of the analysis that justify such determination; or *[Reference: 45 C.F.R. § 164.514(a)]*

3.1.7.2 IDENTIFIERS	The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed: (a) Names; (b) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (i) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (ii) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000. (c) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (d) Telephone numbers; (e) Fax numbers; (f) Electronic mail addresses; (g) Social security numbers; (h) Medical record numbers; (i) Health plan beneficiary numbers; (j) Account numbers; (k) Certificate/license numbers; (l) Vehicle identifiers and serial numbers, including license plate numbers; (m)Device identifiers and serial numbers; (n) Web Universal Resource Locators (URLs); (o) Internet Protocol (IP) address numbers; (p) Biometric identifiers, including finger and voice prints; (q) Full face photographic images and any comparable images; (r) Any other unique identifying number, characteristic, or code, except as permitted for re-identification provided in these guidelines; and *[Reference: 45 C.F.R. § 164.514(b)(12(i)]*
3.1.7.3 RE-IDENTIFICATION	The entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information. *[Reference: 45 C.F.R. § 164.514(b)(2)(ii)]*
3.1.8 Re-	If health information is re-identified, an entity is permitted to use or disclose

Identified Information Use or Disclosure	such re-identified information only as permitted or required by these guidelines. *[Reference: 45 C.F.R. § 164.502(d) & California Privacy and Security Advisory Board Principle 7]* An entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the entity, provided that: (a) *Derivation.* The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and (b) *Security.* The entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification. When an entity discloses de-identified individual health information, the entity shall include a statement to the entity to which the information is being released, that should they re-identify the information, the privacy and security of the resulting individual health information is governed by these guidelines. *[Reference: 45 C.F.R. § 164.514(c) & California Privacy and Security Advisory Board Principle 7]*
3.1.9 Limited Data Set Use or Disclosure	An entity may use or disclose a limited data set only for the purposes of research or public health. An entity may use individual health information to create a limited data set that meets the requirements of this section, or disclose individual health information only to a business associate for such purpose, whether or not the limited data set is to be used by the entity. An entity may use or disclose a limited data set that meets the requirements of the limited data set guidelines, if the entity enters into a data use agreement with the limited data set recipient, in accordance the data use agreement guidelines below. *[Reference: 45 C.F.R. § 164.514(e)(1) & (3)]*
3.1.9.1 LIMITED DATA SET IDENTIFIERS	A limited data set is individual health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (a) Names; (b) Postal address information, other than town or city, state, and zip code; (c) Telephone numbers; (d) Fax numbers; (e) Electronic mail addresses; (f) Social security numbers; (g) Medical record numbers;

	(h) Health plan beneficiary numbers; (i) Account numbers; (j) Certificate/license numbers; (k) Vehicle identifiers and serial numbers, including license plate numbers; (l) Device identifiers and serial numbers; (m)Web Universal Resource Locators (URLs); (n) Internet Protocol (IP) address numbers; (o) Biometric identifiers, including finger and voice prints; and (p) Full face photographic images and any comparable images. *[Reference: 45 C.F.R. § 164.514(e)(2)]*
3.1.9.2 DATA USE AGREEMENTS	An entity may use or disclose a limited data set only if the entity obtains satisfactory assurance, in the form of a data use agreement that meets the requirements of this section, that the limited data set recipient will only use or disclose the individual health information for limited purposes.
3.1.9.3 CONTENTS	A data use agreement between the entity and the limited data set recipient shall: (a) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of these guidelines, if done by the entity; (b) Establish who is permitted to use or receive the limited data set; and (c) Provide that the limited data set recipient will: (i) Not use or further disclose the information other than as permitted by the data use agreement, permitted by these guidelines, or as otherwise required by law; (ii) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement; (iii) Report to the entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware; (iv) Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and (v) Not identify the information or contact the individuals.
3.1.9.4 COMPLIANCE	An entity is not in compliance with this section if the entity knew of a pattern of activity or practice of the limited data set recipient that constituted a material breach or violation of the data use agreement, unless the entity took reasonable steps to cure the breach or end the violation, as applicable, and, if

	such steps were unsuccessful: (a) Discontinued disclosure of individual health information to the recipient; and (b) Reported the problem to the Secretary of U.S. Department of Health and Human Services, the Directors of the California Office of Health Information Integrity, and the California Department of Public Health, as appropriate. An entity that is a limited data set recipient and violates a data use agreement will be in noncompliance with these guidelines. *[Reference: 45 C.F.R. § 164.514(e)(4)]*
3.1.10 Required by Law Use or Disclosure	An entity is permitted to use or disclose individual health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law. For uses and disclosures required by for victims of abuse, neglect, or domestic violence, for judicial or administrative proceedings, or for law enforcement purposes, the entity must meet the guideline requirements. *[Reference: 45 C.F.R. § 164.512(a)]*

3.2 USE AND DISCLOSURE OF INDIVIDUAL HEALTH INFORMATION – HIO AND OTHER ENTITIES	
A health information organization is limited to exchange individual health information as provided in this Section. Other entities are permitted to use and disclose individual health information as provided in this Section and in Section 3.3. *[Reference: California Privacy and Security Advisory Board Vision and Mission Statement, Principles 3d, & 5]*	
3.2.1 Treatment Purpose	A health information organization or two organizations that transmit individual health information electronically are permitted to exchange individual health information on behalf of an entity purposes of:
3.2.1.1 CLINICAL TREATMENT	Clinical treatment, which includes: (i) Health care services provided by a licensed health care professional consisting of diagnosis and rendering care within the scope and practice permitted under law. Such use or disclosure may be limited to the individual health information necessary for the purpose for which the individual is seeking treatment. *[Reference: California Civil Code 56.10(c)(1), 45 C.F.R. 164.501 Definition of Treatment, 164.502(a)(1)(ii), 164.506(c)(2)]*
3.2.2 Public Health Disclosure	Mandated public health reporting, including:
3.2.2.1 PUBLIC HEALTH	A health care provider is permitted to disclose a case or suspected case of any diseases identified by the California Department of Public Health [17 California Administrative Code § 2500(j)] to the local public health officer for the jurisdiction where the individual resides if the provider is attending the case. A health information organization is permitted to exchange on behalf of a provider the above disclosures. *[Reference: California Civil Code § 56.30, California Health and Safety Code § 120130, & 17 California Administrative Code § 2500, 45 C.F.R. § 164.203(c)]*
3.2.2.2 DISEASE CONTROL	A health information organization is permitted to exchange individual health information on behalf of an entity or an entity is permitted to disclose individual health information for the public health activities and purposes as permitted by state and federal law or regulation, to a public health authority for the purpose of: ▪ For preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and

	▪ For conducting public health surveillance, investigations, and interventions. *[Reference: California Civil Code § 56.10(c)(18) & 45 C.F.R. §§ 164.203(c), & 164.512(b)(1)(i)]*
3.2.2.3 INDIVIDUAL WITH DISEASE	A health information organization is permitted to exchange individual health information on behalf of an entity or an entity is permitted to disclose individual health information to an authorized government authority to notify a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation. *[Reference: California Civil Code 56.10(c)(18), California Health and Safety Code § 102175 & 45 C.F.R. § 164.512(b)(1)(iv)]*
3.2.2.4 CORONERS AND MEDICAL EXAMINERS	A health information organization is permitted to exchange individual health information on behalf of an entity or an entity shall disclose individual health information to a coroner or medical examiner when requested in the course of an investigation by the coroner's office for the purposes of: (a) Identifying the decedent or locating next of kin, or (b) When investigating deaths that may involve: (i) Public health concerns, (ii) Organ or tissue donations, (iii) Child abuse, (iv) Elder abuse, (v) Suicides, (vi) Poisonings, (vii) Accidents, (viii) Sudden infant deaths, (ix) Suspicious deaths, (x) Unknown deaths, or (xi) Criminal deaths, or (xii) When otherwise authorized by the decedent's representative. Individual health information requested by the coroner shall be limited to information regarding the patient who is the decedent and who is the subject of the investigation and shall be disclosed to the coroner without delay upon request. An entity that also performs the duties of a coroner or medical examiner may use individual health information for the purposes described in this paragraph. *[Reference: California Civil Code § 56.10(b)(8), § 56.10(c)(6) & 45 C.F.R. §*

	164.512(g)(1)]
3.2.4 Disaster Relief Use or Disclosure	A health information organization is permitted to exchange individual health information on behalf of an entity, or an entity is permitted to use or disclose individual health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted for notification of a family member, personal representative, or individual responsible for the care of the individual. The requirements when the individual is present or not present apply to such uses and disclosure to the extent that the entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances. *[Reference: California Civil Code § 56.1007(e) & 45 C.F.R. § 164.510(b)(4)]*

3.3 USE AND DISCLOSURE OF INDIVIDUAL HEALTH INFORMATION – ALL OTHER ENTITIES

Entities that utilize or access electronic health information exchange, except for health information organizations shall comply with this section.

The electronic transmission of individual health information is limited to specific purposes (see Section 3.2), and participants may not be able to segregate the individual health information obtained through an electronic health information exchange from individual health information otherwise obtained. Therefore, entities shall assist in the California Privacy and Security Advisory Board development of access controls and other privacy and security measures for the limited purpose of the exchange, while not limiting the other uses of individual health information which are required or permitted under law, i.e., the Health Insurance Portability and Accountability Act (HIPAA), the California Confidentiality of Medical Information Act, etc.

An entity, other than a health information organization, is permitted to use or disclose individual health information for the purposes listed in Section 3.2 and the following purposes.

3.3.1 Treatment Use or Disclosure	An entity, not including a health information organization, is permitted to request, use, or disclose individual health information for:
3.2.1.1 CLINICAL TREATMENT	(a) Its own treatment purposes. An entity, not including a health information organization, is permitted to disclose individual health information for treatment activities of a health care provider. *(See Section x)* *[Reference: 45 C.F.R. §§ 164.502(a)(1)(ii), 164.506(a) & 164.506(c)(1) & (2), California Civil Code § 56.10(c)(1)]*
3.2.1.2 CARE MANAGEMENT	(b) Care management, which includes assistance provided to patients to provide and support health and wellness which includes the following types of activities:
3.2.1.2.1 Administration of Care	(i) Assist a patient with the administration of his/her health care including: (A) Internal administration, such as scheduling appointments, coordinating staff, (B) Transferring health records to a specialist (C) Transmitting prescription/laboratory requests and test results to health care providers (D) Ensuring health plan coverage for proposed services.
3.2.1.2.2 Multiple Services	(ii) Coordinate the provision of multiple health care services to a patient including: (A) Discharge planning, (B) Sharing current medical records with a team of health care providers rending health care in a home setting, (C) Transmitting prescription/laboratory requests and test results to

	the team of health care providers overseeing the individual's care (D) Sharing medical records with multi-disciplinary team members for planning the patient's care.
3.2.1.2.3 Plan of Care	(iii) Support a patient in following a plan of health care (A) Chronic/disease care management (B) Continuity of care (C) Coordination of care
3.3.2 Payment Use or Disclosure	An entity, not including a health information organization, is permitted to request, use, or disclose individual health information for its own payment purposes. An entity, not including a health information organization, is permitted to disclose individual health information to another entity or health care provider to the extent necessary to allow responsibility for payment to be determined and payment to be made by the entity that receives the information. *[Reference: 45 C.F.R. §§ 164.502(a)(1)(ii) & 164.506(c)(3), California Civil Code § 56.10(c)(2)]*
3.3.3 Health Care Operations Use or Disclosure	An entity may disclose individual health information for the health care operations of a healthcare provider or health plan *(see definition of health care operations)* to: (a) The health plan or health care provider (or their representatives) that have a current relationship with the individual who is the subject of the individual health information being requested; (b) The individual health information pertains to such relationship, and (c) The disclosure is for one of the following activities permitted under these guidelines. *[Reference: 45 C.F.R. §§ 164.502(a)(1)(ii) & 164.506(c)(3), California Civil Code § 56.10(c)(3) & § 56.10(c)(4) & § 56.10(c(5)]*
3.3.4 Business Associate Use or Disclosure	An entity is permitted to disclose individual health information pursuant to a business associate agreement. An entity is permitted to disclose individual health information to a business associate and may allow a business associate to create or receive individual health information on the entities behalf, if the entity obtains satisfactory assurance that the business associate will appropriately safeguard the information and the purpose is consistent with California laws. *[Reference: 45 C.F.R. § 164.502(e)(1)*
3.3.4.1 EXCEPTIONS	This does not apply to: (a) Disclosures by an entity to a health care provider concerning the treatment of the individual;

	(b) Disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the requirements of these guidelines and are met; or (c) Uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the individual health information used to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of individually health information for the performance of such functions by the health plan and the agency other than the agency administering the health plan. *[Reference: 45 C.F.R. § 164.502(e)(1)]*
3.3.5 Public Health	If the entity also is a public health authority, the entity is permitted to: (a) Disclose information, as permitted by state and federal law or regulation, to public health authorities for the purpose of: (i) Preventing or controlling disease, injury, or disability including but not limited to, (A) The reporting of disease, injury, vital events including but not limited to birth or death; and (ii) The conducting of public health surveillance, public health investigations and public health interventions as authorized by state or federal law or regulation. *[Reference: 45 C.F.R. § 164.512(b)(2)]*
3.3.5.1 PUBLIC HEALTH AUTHORITY REDISCLOSURE	Public health contractors or other persons or entities to which a public health authority has granted authority to act pursuant to a contract, grant, cooperative agreement, or memoranda of understanding shall not redisclose individual health information unless it is expressly permitted under their grant of authority. *[Reference: California Civil Code § 56.30, California Health and Safety Code § 120130, & 17 California Administrative Code § 2500, 45 C.F.R. § 164.203(c)]*
3.3.5.2 FDA-REGULATED PRODUCTS	An entity is permitted to disclose individual health information to another entity that is subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product. Such purposes include: (a) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations; (b) To track FDA-regulated products;

	(c) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or (d) To conduct post marketing surveillance. *[Reference: 45 C.F.R. § 164.512(b)(iii)]*
3.3.5.3 FDA ACTIVITIES	An entity may disclose individual health information to another entity that has responsibility for activities related to the quality, safety, or effectiveness of such FDA-regulated product or activity. Such purposes include: (e) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations; (f) To track FDA-regulated products; (g) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or To conduct post marketing surveillance. *[Reference: 45 C.F.R. § 164.512(b)(iii)]*
3.3.6 Employers	If the entity also is a public health authority, the entity is permitted to use individual health information in all cases in which it is permitted to disclose such information for public health activities as described in these guidelines. *[Reference: 45 C.F.R. § 164.512(b)(2)]*
3.3.6.1 SUMMARY HEALTH INFORMATION	An entity, not including a health information organization, is permitted to disclose to an employer, summary health information which does not disclose individual health information about an individual who is a member of the workforce of the employer, for the purposes of: (a) Obtaining premium bids from health plans for providing health insurance coverage under the group health plan; or (b) Modifying, amending, or terminating the group health plan.
3.3.6.2 EMPLOYMENT RELATED HEALTH CARE	An entity is permitted to disclose individual health information to an employer concerning a member of the workforce of such employer or who provides health care to the individual at the request of the employer, when the individual health information was created as a result of employment-related health care services to an employee conducted at the specific prior written request and expense of the employer: (a) To evaluate whether a person has a work related injury or illness, or (b) The individual health information that is disclosed consists of functional limitations and fitness to perform work duties.
3.3.6.3 EMPLOYMENT	An entity, not including a health information organization, may disclose to an employer concerning a member of the workforce of such employeror

RELATED INJURY OR ILLNESS	who provides health care to the individual at the request of the employer when the individual health information was created as a result of employment-related health care services to an employee conducted at the specific prior written request and expense of the employer: (a) To conduct an evaluation relating to medical surveillance of the workplace, (b) The individual health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related illness or injury or a workplace-related medical surveillance, (c) The employer needs such findings to comply with its obligations under 29 C.F.R. Parts 1904 through 1928, 30 C.F.R. Parts 50 through 90 [Federal Occupational Health and Safety; investigation of work-related deaths, etc.], or state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and (d) The health care provider provides written notice to the individual that his/her health information relating to the medical surveillance of the workplace and work-related illness and injuries is disclosed to the employer..
3.3.7 Health and Safety Use or Disclosure	
3.3.7.1 DISCLOSURE BY PSYCHOTHERAPIST FOR HEALTH AND SAFETY	A health information organization is permitted to exchange individual health information on behalf of a psychotherapist *(as defined in Section 1010 of the Evidence Code)* consistent with applicable law and standards of ethical conduct, if the psychotherapist, in good faith, believes the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a reasonably foreseeable victim or victims, and the disclosure is made to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat. *[California Civil Code § 56.10(c)(19) & 45 C.F.R. § 164.512(j)]*
3.3.7.2 DISCLOSURES TO A CONSERVATORSHIP	A health information organization is permitted to exchange individual health information on behalf of an entity, or an entity is permitted to disclose individual health information relevant to an individual's condition, care, treatment provided to a probate court investigator required or authorized in a conservatorship proceeding or to a probate court investigator, probation officer, or domestic relations investigator, probation officer, or domestic relations investigator engaged in determining the need for an additional guardianship or continuation of an existing guardianship. *[Reference: California Civil Code § 56.10(c)(12)]*
3.3.8 Health Care Oversight Use	If an entity also is a health oversight agency, the entity may use or disclose individual health information for the purpose of health oversight activities to a health oversight entity, in accordance with state law pertaining to such oversight entity.

	(Reference: California Civil Code §§56.10(c)(4) & (c(5), California Penal Code §§1543 & 1545; California Government Code § 11180(g); 45 C.F.R. § 164.512(a), 164.512(d)(4), & 164.512(e)]
3.3.9 Judicial and Administrative Proceedings Use or Disclosure	The guidelines for disclosures for purposes of judicial and administrative proceedings do not supersede other provisions of this section that otherwise permit or restrict uses or disclosures of individual health information. *[Reference: 45 C.F.R. § 164.512(e)(2)]*
3.3.9.1 JUDICIAL AND ADMINISTRATIVE PROCEEDINGS DISCLOSURE	An entity shall disclose individual health information if the disclosure is compelled by any of the following: (a) By a court pursuant to an order of that court. (b) By a board, commission, or administrative agency for purposes of adjudication pursuant to its lawful authority. (c) Consistent with Section 1985.3 of the California Code of Civil Procedure, by a party to a proceeding before a court or administrative agency pursuant to subpoena, subpoena duces tecum, notice to appear served pursuant to Section 1987 of the Code of Civil Procedures, or any provision authorizing discovery in a proceeding before a court or administrative agency. (d) Consistent with Section 1985.3 of the California Code of Civil Procedure, by a board, commission, or administrative agency pursuant to an investigative subpoena issued under Article 2 (commencing with Section 11180) of Chapter 2 of Part 1 of Division 3 of Title 1 of the Government Code. (e) By an arbitrator or arbitration panel, when arbitration is lawfully requested by either party, pursuant to a subpoena duces tecum issued under Section 1282.5 of the California Code of Civil Procedure, or another provision authorizing discovery in a proceeding before an arbitrator or arbitration panel. (f) By a search warrant lawfully issued to a governmental law enforcement agency. *[Reference: California Civil Code § 56.19(b)(1-6), California Code of Civil Procedures § 1983.5, & 45 C.F.R. § 164.512(e)]*
3.3.10 Law Enforcement	Entities are permitted to disclose individual health information for the purpose of law enforcement in accordance with state law pertaining to such law enforcement entity. *[Reference: California Civil Code § 56.30(g), California Penal Code § 1543, & 45 C.F.R. § 164.512(f)]*
3.3.10.1 Required by Law	An entity, not including a health information organization, may disclose individual health information: (c) As required by law including laws that require the reporting of certain

	types of wounds or other physical injuries, except for laws related to reporting of child abuse, abuse, neglect or domestic violence; or (d) In compliance with and as limited by the relevant requirements of: (i) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer; (ii) A grand jury subpoena; or (iii) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that: (A) The information sought is relevant and material to a legitimate law enforcement inquiry; (B) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and (C) De-identified information could not reasonably be used. *[Reference: California Civil Code § 56.30(g), California Penal Code § 1543, & 45 C.F.R. § 164.512(f)(1)]*
3.3.11 Victims of Abuse	An entity that is required to report is permitted to disclose individual health information for the purposes of reporting suspected child abuse or neglect to the appropriate state and local agencies. *[Reference: California Civil Code § 56.30(g) & 45 C.F.R. § 164.512(f)]*
3.3.12 Victims of a Crime – Decedents	A health care provider shall disclose individual health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if the entity reasonably suspects that such death may have resulted from criminal conduct. *[Reference: California Penal Code § 11160 & 45 C.F.R. § 164.512(f)(4)]*
3.3.13 Decedents Disclosure	
3.3.13.1 FUNERAL DIRECTORS	In the event of the demise of the person afflicted with the reportable disease or condition, a health facility or county health officer shall notify the funeral director, charged with removing the decedent from the health facility, of the reportable disease prior to the release of the decedent from the health facility to the funeral director. *[Reference: California Health and Safety Code § 1797.188(c), California Civil Code § 56.10(b)(8), § 56.10(c)(6) & 45 C.F.R. § 164.512(g)(2)]*
3.3.13.2 CORONERS OR MEDICAL EXAMINERS	An entity is permitted to disclose individual health information to a coroner or medical examiner for the purposes of identifying a deceased person, determining a cause of death, or other duties as authorized by law. A covered entity that also performs the duties of a coroner or medical examiner is permitted to use individual health information for the purposes

	described in this paragraph. *[Reference: California Civil Code §§ 56.10(b)(8) & (c)(6), California Health and Safety Code § 1797.188, & 45 C.F.R. § 164.512(g)]*
3.3.14 Cadaveric Organ, Eye, Tissue Use or Disclosure	A provider of health care or a health care service plan is permitted to disclose individual health information to an organ procurement organization or tissue bank processing the tissue of a decedent for transplantation into the body of another person, but only with respect to the donating decedent, for the purpose of aiding the transplant. For purposes of this paragraph "tissue bank" and "tissue" have the same meanings as defined in Section 1635 of the California Health and Safety Code. *[Reference: California Civil Code § 56.10(c)(13) & 45 C.F.R. § 164.512(h)]*
3.3.15 Government Functions	
3.3.15.1 CORRECTIONAL INSTITUTIONS AND OTHER CUSTODIAL SITUATIONS	An entity that is required by to report individual health information for purposes of aiding correctional law enforcement officers may disclose such information. For the purposes of this provision, an individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody. *[Reference: California Civil Code § 56.10,§ 56.10(c)(19) § 56.30, & (45 C.F.R. § 164.512(k)(5)]*
3.3.15.2 GOVERNMENT PROGRAMS PROVIDING PUBLIC BENEFITS	Entities are permitted to disclose individual health information for the purpose of government programs providing public benefits in accordance with state law pertaining to such government program. *[Reference: California Civil Code § 56.30(b), California Penal Code § 1543e) & 45 C.F.R. § 164.512(k)(6)]*
3.3.16 Plan Sponsors Use and Disclosure	An entity is permitted to disclose summary health information to a plan sponsor which does not disclose individual health information for the purpose of: (a) Obtaining premium bids from health plans for providing health insurance coverage under a group health plan; or (b) Modifying, amending, or terminating the group health plan. A group health plan sponsor may enter into an agreement with a health plan for the disclosure of additional information, consistent with 45 C.F.R. § 164.504(f), subject to more stringent State law. *[Reference: California Civil Code § 56.10(c)(9) & 45 C.F.R. § 164.504(f)]*
3.3.17 Underwriting Use or Disclosure Limitation	An entity may not use individual health information for underwriting unless the services were paid for by insurance company in a specific circumstance consistent with California Civil Code § 56.10(c)(9) or 56.10(c)(11). If the underwriting has to do with re-insurance, the entity is required to disclose only data that is de-identified if disclosed to a plan sponsor. An entity with

	the responsibility to pay for services rendered is permitted to have access to the individual health information only to the extent necessary to allow for the responsibility for payment to be determined. *[Reference: California Civil Code § 56.10(c)(2), (c)(9), & (d) & 45 C.F.R. § 164.01 definition of health care operations (3) & 164.514(g)]*
3.3.18 Worker's Compensation	Subject to more stringent State law, an entity, not including a health information organization, may disclose individual health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault. *[Reference: California Civil Code § 56.30(e), (f), & (h) & 45 C.F.R. § 164.512(l)]*
3.3.19 Marketing	
3.3.19.1 MARKETING INCLUDES	Marketing is to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.
3.3.19.2 MARKETING EXCLUDES	An entity shall obtain an authorization for any use or disclosure of individual health information for marketing, except for a communication that is from an entity that has an existing relationship with the individual, without remuneration, either direct or indirect, and is for any of the following purposes: (a) For treatment of the individual' (b) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual; or (c) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about (i) Replacement of, or enhancements to a health plan (ii) Health-related products or services available only to a health plan. [*Reference: 45 C.F.R. § 164.501, 164.506(a)(3), HITECH, Section 13406, California Civil Code § 56.05 & 56.10(d)]*
3.3.20 Psychotherapy Notes	An entity is permitted to disclose individual health information regarding mental health treatment only in accordance with state and federal law pertaining to such information. *[Reference: California Welfare and Institutions Code § 5328, California Civil Code § 56.104, & 45 C.F.R. 164.508]*
3.3.21 HIV	An entity is permitted to disclose individual health information regarding HIV

	status only in accordance with state and federal law pertaining to such information. *[Reference: California Civil Code § 56.31]*
3.3.22 Research Use or Disclosure	An entity is permitted to disclose individual health information to public agencies, clinical investigators, including investigators conducting epidemiological studies, health care research organizations, and accredited public or private nonprofit educational or health care institutions for bona fide research purposes provided that: *[Reference: 45 C.F.R. § 164.512(i)(1) & California Civil Code§ 56.10(c)(7)]*
3.3.22.1 -BOARD APPROVAL OF WAIVER	The entity obtains documentation that an alteration to or waiver, in whole or in part, of a valid individual authorization required by these guidelines for use or disclosure of individual health information has been approved by either:
3.3.22.2 -IRB	An Institutional Review Board (IRB), established in accordance with federal regulations.[4]; or
3.3.22.3 PRIVACY BOARD	A privacy board that: (a) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests; (b) Includes at least one member who is not affiliated with the entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and (c) Does not have any member participating in a review of any project in which the member has a conflict of interest. *[Reference: 45 C.F.R. § 164.512(i)(1)(i)]*
3.3.22.4 RESEARCH PREPARATION (V1)	When a researcher requests to use individual health information in activities preparatory to research, the entity shall obtain from the researcher representations that: (a) Use or disclosure is sought solely to review individual health information as necessary to prepare a research protocol or for similar purposes preparatory to research; (b) No individual health information is to be removed from the covered entity by the researcher in the course of the review; and (c) The individual health information for which use or access is sought is necessary for the research purposes. *[Reference: 45 C.F.R. § 164.512(i)(1)(ii)]*
3.3.22.5 -DECEDENT	When a researcher requests to use individual health information in

[4] 7 CFR lc.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107

INFORMATION	activities related to a decedent, the entity shall obtain from the researcher: (a) Representation that the use or disclosure sought is solely for research on the individual health information of decedents; (b) Documentation, at the request of the covered entity, of the death of such individuals; and (c) Representation that the individual health information for which use or disclosure is sought is necessary for the research purposes. *[Reference: 45 C.F.R. § 164.512(i)(1)(iii)]*
3.3.22.6 DOCUMENTATION OF WAIVERS	For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, the documentation must include all of the following: *[Reference: 45 C.F.R. § 164.512(i)(2)]*
3.3.22.6.1 IDENTIFICATION AND DATE OF ACTION	(a) A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved; *[Reference: 45 C.F.R. § 164.512(i)(2)(i)]*
3.3.22.6.2 WAIVER CRITERIA	(b) A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria: (i) The use or disclosure of individual health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements; (A) An adequate plan to protect the identifiers from improper use and disclosure; (B) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and (C) Adequate written assurances that the individual health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of individual health information would be permitted by this subpart; (ii) The research could not practicably be conducted without the waiver or alteration; and (iii) The research could not practicably be conducted without access to and use of the individual health information. *[Reference: 45 C.F.R. § 164.512(i)(2)(ii)]*
3.3.22.6.3	(c) A brief description of the individual health information for which use or

INDIVIDUAL HEALTH INFORMATION NEEDED	access has been determined to be necessary by the IRB or privacy board has determined, as the research could not practicably conducted without access to and use of the individual health information. *[Reference: 45 C.F.R. § 164.512(i)(2)(iii)]*
3.3.22.6.4 REVIEW AND APPROVAL PROCEDURES	(d) A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows: (i) An IRB must follow the requirements of the Common Rule, including the normal review procedures[5]; (ii) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who is not affiliated with the entity, with any entity conducting or sponsoring the research and not related to any person who is affiliated wit any of such, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure; (iii) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the individual health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair; and *[Reference: 45 C.F.R. § 164.512(i)(2)(iv)]*
3.3.22.6.5 REQUIRED SIGNATURE	(e) The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable. *[Reference: 45 C.F.R. § 164.512(i)(2)(v)]*
3.3.23.7 REDISCLOSURE	A recipient of individual health information for research purposes shall not further disclose individual health information previously disclosed for that purpose. In the case of research, individual health information used for the purposes of research shall not be further disclosed. *[Reference: California Civil Code §56.10(c)(7)]*

[5] (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR 11.110)

3.3.24 Facility Directories	A health care provider is permitted to disclose individual health information for purposes of facility directories of general acute care hospitals, except where an objection is expressed by the individual. (a) The individual health information disclosed to the facilities directory of general acute care hospitals is limited to: (i) The individual's name, (ii) The individual's location in the general acute care hospital, (iii) The individual's condition described in general terms that does not communicate specific medical information about the individual, and (iv) The individual's religious affiliation. (b) The information may be disclose only to: (v) Members of the clergy, or (vi) Except for religious affiliation, to other persons who ask for the individual by name. (c) A health care provider must inform an individual of the individual health information that it may include in a facilities directory of general acute care hospitals and the persons to whom it may disclose such information (including disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by paragraph (a)(1) of this section. (d) If the opportunity to object to uses or disclosures cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, a health care provider may use or disclose some or all of the individual health information permitted for the facility's directory of general acute care hospitals, if such disclosure is: (vii) Consistent with a prior expressed preference of the individual, if any, that is known to the covered health care provider; and (viii) In the individual's best interest as determined by the health care provider, in the exercise of professional judgment. (e) The health care provider must inform the individual and provide an opportunity to object to uses or disclosures for directory purposes as when it becomes practicable to do so. *[Reference: California Civil Code § 56.10(c)(16) & 45 C.F.R. § 164.510(a)]*

4.1 POLICIES AND PROCEDURES

An entity shall implement policies and procedures with respect to individual health information that are designed to document compliance with these guidelines. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to individual health information undertaken by the entity, to ensure such compliance.

[Reference: 45 C.F.R. § 164.530 (i) Standard: policies and procedures, 45 C.F.R § 164.316 (a) – Standard: Policies and Procedures]

4.1.1 Documentation of Policies and Procedures	An entity shall implement and maintain the policies and procedures required by the privacy and security guidelines in written or electronic form. Each entity shall comply with the following: (a) In deciding which privacy and security measures to use, an entity shall take into account the following factors: (i) The size, complexity, and capabilities of the entity. (ii) The entity's technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures. (iv) The probability and criticality of potential risks to individual health information. (b) The policy and procedures are not to be construed to permit or excuse an action that violates any other requirement of these guidelines. (c) An entity must retain the documentation of the policies and procedures for six years from the date of its creation or the date when it last was in effect, whichever is later. *(See section 4.4)* *[Reference: 45 C.F.R § 164.316 (a) & 45 C.F.R. § 164.530(j)(2)]*
4.1.2 Changes to Policies	An entity shall change its policies and procedures as necessary and appropriate to comply with changes in the guidelines. When an entity changes a privacy practice that is stated in the notice of privacy practices to individuals *(See section 2.2),* and makes corresponding changes to its policies and procedures, it may make the changes effective for individual health information that it created or received prior to the effective date of the notice revision: (a) If the entity has included in the notice to individuals a statement reserving its right to make such a change in its privacy practices; OR (b) An entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented and do not materially affect the content of the notice of privacy practices to individuals.

	[Reference: 45 C.F.R. § 164.530 (i)(2)]
4.1.3 Change in Law	Whenever there is a change in law that necessitates a change to the entity's policies or procedures, the entity shall promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the notice of privacy practices to individuals *(see section 2.2)* the entity must promptly make the appropriate revisions to the notice of privacy practices. *[Reference: 45 C.F.R. § 164.530 (i)(3)]*
4.1.4 Changes to Business Practice	(a) To implement a change as stated in section 4.1.2, an entity must: (i) Ensure that the policy or procedure, as revised to reflect a change in the entity's privacy practice as stated in its notice of privacy practices *(see section 2.2)* complies with the guidelines; (ii) Document the policy or procedure, as revised; and (iii) Revise the notice of privacy practices to state the changed practice and make the revised notice available. (b) The entity shall not implement a change to a policy or procedure prior to the effective date of the revised notice. (c) If an entity has not reserved its right to change a privacy practice that is stated in the notice of privacy policies, the entity is bound by the privacy practices as stated in the notice with respect to individual health information created or received while such notice is in effect. *[Reference: 45 C.F.R. § 164.530 (i)(4)]*

4.2 PERSONNEL DESIGNATION

An entity shall designate a person or office that is responsible for the development and implementation of the privacy and security policies and procedures of the entity.

[References: 45 C.F.R. §164.530(a) (2), 45 C.F.R § 164.308 (a)(2)]

4.2.1 Designated Officials	Each entity shall identify the entity's primary privacy and primary security person or office that is responsible for implementation and compliance to the privacy and security guidelines, respectively. Nothing prevents an entity from appointing the same individual to serve both official roles. *[Reference: 45 C.F.R. §§ 164.308(a)(2) & 164.530(a)(1)(i)]*
4.2.2 Privacy Responsibilities	An entity shall designate a person or office that is responsible for the development and implementation of the privacy policies and procedures of the entity. *(See sections 1.0-4.0)* *[Reference: 45 C.F.R. §§ 164.530(a)(1)(i) & 164.530(i)]*
4.2.3 Security	An entity shall designate a person or office that is responsible for the development and implementation of the security policies and procedures

Responsibilities	required by these *guidelines (see sections 4.0 through 8.0).* *[Reference: 45 C.F.R. § 164.308(a)(2)]*
4.2.4 Complaints	An entity shall identify an individual or office that is designated to handle complaints and respond to inquiries about the entity's notice of privacy practices. *(See Sections 2.2 and 4.6)* *[Reference: 45 C.F.R. § 164.530(a)(1)(ii)]*
4.2.5 Access	An entity shall designate a person or office responsible for receiving or processing requests for access to individual health information by an individual or his/her authorized representative. *(See Section 2.4)* *[Reference: 45 C.F.R. § 164.524(e)]*
4.2.6 Amendments	An entity shall designate a person or office to which an individual may request access to amendments to his/her individual health information. *(See Section 2.5)* *[Reference: 45 C.F.R. § 164.526(f)]*
4.2.7 Accounting of Disclosures	An entity shall designate a person or office to which an individual may request an accounting of disclosures of his/her individual health information. *(See Section 2.6)* *[Reference: 45 C.F.R. § 164.528(d)(3)]*
4.2.8 Documentation	An entity shall document *(see Section 4.4)* the personnel designations as required by this section *[Reference: 45 C.F.R. § 164.530(j)(1)(iii)]*

4.3 VERIFICATION OF IDENTITY

An entity shall verify the identity and authority of individuals and other entities requesting access to individual health information.

[References: 45 C.F.R. § 164.514(h)]

4.3.1 Requestors to be Verified	Prior to any disclosure permitted by these guidelines, an entity shall: (a) Verify the identity of a person requesting individual health information if the identity or authority of such person is not known to the entity. except with respect to disclosures: (i) For facility directories *(see Section 3.6.9)* (ii) To persons involved in the care of an individual *(see Section 3.6.13)* and (iii) For disaster relief purposes *(see Section 3.6.14).* (b) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the individual health information as

	a condition of the disclosure under these guidelines. [*Reference: 45 C.F.R. § 164.514(h)(1) & (2)]*
4.3.1.1 CONDITIONS OF DISCLOSURES	If a disclosure is conditioned on particular documentation, statements, or representations from the person requesting the individual health information, an entity may reasonably rely on documentation, statements, or representations that meet the applicable requirements. (a) The conditions as required by law to disclose individual health information to law enforcement *(see section 3.3.10)* may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met. (b) The documentation required to disclose individual health information for research *(see section 3.3.22)* shall satisfy the criteria and be dated and signed in accordance with the requirements to disclose individual health information for research purposes. *[Reference: 45 C.F.R. § 164.514(h)(2)(i) 45 C.F.R. § 164.512(i)(2) & 45 C.F.R. § 164.512(f)]*
4.3.1.2 IDENTITY OF PUBLIC OFFICIALS	An entity may reasonably rely on any of the following to verify identity when the disclosure of individual health information is to a public official or a person acting on behalf of the public official. (a) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status; (b) If the request is in writing, the request is on the appropriate government letterhead; or *(c)* If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official. *[Reference: 45 C.F.R. § 164.514(h)(2)(ii)]*
4.3.1.3 AUTHORITY OF PUBLIC OFFICIALS	An entity may reasonably rely on any of the following to verify authority when the disclosure of individual health information is to a public official or a person acting on behalf of the public official. (a) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority; (b) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority. *[Reference: 45 C.F.R. § 164.514(h)(2)(iii)]*

4.3.1.4 EXERCISE OF PROFESSIONAL JUDGMENT	The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure ~~(a) For facility directories (see section 3.6.9)~~ ~~(b) To persons involved in the care of an individual (see section 3.6.13) and~~ (a) For disaster relief purposes (see section 3.2.4), or (b) Acts on a good faith belief in making a disclosure to prevent or lessen a serious and imminent threat to the health or safety of a person or the public (see section 3.3.7). *[Reference: 45 C.F.R. § 164.514(h)(2)(iv)]*
4.3.2 Entity Personnel (Users)	An entity shall establish policies and procedures to verify the identity of entity personnel and other users of the entity's systems. *[Reference: 45 C.F.R. § 164.514(h) and 164.530(i)]*
4.3.3 Individual Access to Records	An entity shall verify the identity of individuals requesting access to his/her individual health information. Before disclosing the individual health information to an personal representative of the individual requesting access to the individual health information, the entity shall verify: (a) The identity of the personal representative using a government-issued photo identification, (b) Their legal authority to act on behalf of the individual, (c) And, if appropriate, the limitations of their authority. *[Reference: 2.1.1 – 2.1.3 California Privacy and Security Advisory Board Verification of ID Task Group and Survey]*
4.3.4 Reasonable Verification	An entity that receives requests for access to individual health information shall verify the identity of the requestor by reviewing government-issued photo identification. Where a government issued photo identification is not available, the entity may use two or more documents that provide identifying information about the individual. When the individual is representing an entity, the entity shall review an official document from the requesting entity authorizing the individual to request the disclosure. An entity can require reasonable verification of identity prior to permitting inspection or copying of a patient's records, so long as this requirement is not used oppressively or discriminatorily to frustrate or delay compliance with access to records. *[Reference: California Health and Safety Code § 123110(g)]*
4.3.5 Identification of Patients [NEW]	Health care providers shall identify patients to appropriately collect and maintain individual health information. Health care providers may use the following primary factors for patient identification purposes. Health care providers may use the secondary factors when the patient's identity cannot be established using the primary factors. Health care providers may use the tertiary factors when the patient's identity cannot be established using the

	primary and secondary factors. [*Reference: 2.1.1 – 2.1.3 California Privacy and Security Advisory Board Verification of ID Task Group and Survey]*
4.3.5.1 PRIMARY PATIENT IDENTIFICATION FACTORS	(a) Name of the Patient (b) Date of Birth of the Patient (c) ID Number of the Patient. This may include, but is not limited to, health insurance numbers, state drivers' license numbers, state identification numbers, etc. (d) Address of the Patient *[Reference: California Health and Safety Code § 123110(g)]*
4.3.5.2 SECONDARY PATIENT IDENTIFICATION FACTORS	(a) Telephone or Cell Phone Numbers of the Patient (b) Place of Birth of the Patient (c) Emergency Contact (Spouse, Next of Kin, etc.) for the Patient
4.3.5.3 TERTIARY PATIENT IDENTIFICATION FACTORS	(a) Email Address of the Patient (b) Mother's Maiden Name of the Patient (c) Also Known As Name(s) of the Patient

4.4 DOCUMENTATION AND RETENTION

An entity shall document the implementation and maintenance of its privacy and security activities required by the guidelines. Such documentation will provide evidence of compliance.

[Reference: 45 C.F.R. § 164.530(j)]

4.4.1 Required Documentation	(a) An entity shall: (i) Maintain the policies and procedures required by the privacy and security guidelines in written or electronic form; (ii) Maintain documentation in writing or an electronic copy if a communication is required by the privacy and security guidelines to be in writing; and (iii) Maintain a written or electronic record of such action, activity, or designation if an action, activity, or designation is required by the privacy and security guidelines to be documented. *[Reference: 45 C.F.R. § 164.530 (j)(1) & § 164.316(b)(1)]* (b) Documentation includes, but is not limited to documentation of: (i) HIEconsent *(see Section 2.1)* (ii) Notice of Privacy Practices *[45 C.F.R. § 164.520]* (iii) Business Associate Contracts *[45 C.F.R. § 164.502 (e)(2)]*

	(iv) Authorizations of Disclosures of Individual Health Information *[45 C.F.R. § 164.508 (b)(6)]* (v) Disclosures for Judicial and Administrative Hearings *[45 C.F.R. § 164.512(e)(1)]* (vi) Documentation of Notice to Employees *[45 C.F.R. § 164.512(b)(v)(D)]* (vii) Research *[45 C.F.R. § 164.512 (i)(1)]* (viii) Verification of Identity *[45 C.F.R. § 164.514 (h)(1)]* (ix) Restriction *[45 C.F.R. § 164.522 (a)(3)]* (x) Access *[45 C.F.R. § 164.524 (e)]* (xi) Amendment *[45 C.F.R. § 164.526 (f)]* (xii) Accounting of Disclosures *[45 C.F.R. § 164.528 (d)]* (xiii) Complaints *[45 C.F.R. § 164.530 (d)(2)]* (xiv) Sanctions *[45 C.F.R. § 164.530 (e)(2)]* (xv) Security Awareness and Training *[45 C.F.R. § 164.308(a)(5)]* (xvi) Security Incident Reports *[45 C.F.R. § 164.308(a)(6)]* (xvii) Testing and Revision of Contingency Plans *[45 C.F.R. § 164.308(a)(7)*] (xviii) Results of Evaluation of Policy and Technical *Compliance [45 C.F.R. § 164.308(a)(8)]* (xix) Workforce Sanctions *[45 C.F.R. §§ 164.308(a)(1)(ii)(C) & 164.530(e)(1)]* (xx) Operating Systems and Database Hardening/Patch Management *[NIST SP 800-123 (Section 4)]* (xxi) Audit Controls and Considerations *[45 C.F.R. § 164.312(b)*
4.4.2 No Documentation Required	An entity is not required to document information considered de-identified data. *(see section 3.1.7)* *[Reference: California Privacy and Security Advisory Board]*
4.4.3 Retention Period	(a) An entity shall retain the documentation required by these guidelines for six years from the date of its creation or the date when it last was in effect, whichever is later. *[Reference: 45 C.F.R. § 164.530 (j)(2)]* (b) Providers of health services have an obligation to preserve medical records for a minimum of seven (7) years following discharge of the patient, except that the record of unemancipated minors shall be kept at least one year after the minor has reached the age of 18 years, and in any case, no less than seven years. *[Reference: Health and Safety Code § 123145(a)]*

4.4.4 Disposal of Records	Each provider of health care, health care service plan, or contractor that creates, maintains, preserves, stores, abandons, destroys, or disposes of medical records shall do so in a manner that preserves the confidentiality of the information contained therein. *[Reference: Civil Code § 56.101]*

4.5 TRAINING

An entity shall train all members of its workforce on the policies and procedures with respect to individual health information required by these guidelines, as necessary and appropriate for the members of the workforce to carry out their function within the entity.

[*Reference: 45 C.F.R. § 164.530 (b) Training, 45 C.F.R. § 164.308 (a)(5) Security Awareness & Training, ISO 8.2.2 – Information Security Awareness, Education and Training]*

4.5.1 Provision of Training	An entity shall have provided training to each member of the entity's workforce, as relevant to their job function. In addition, an entity shall have provided training as follows: ▪ Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and ▪ To each member of the entity's workforce whose functions are affected by a material change in the policies or procedures as required by these guidelines, within a reasonable period of time after the material change becomes effective. ▪ To appropriate members of the entity's workforce, security awareness updates. Updates shall include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities (e.g. log-on procedure, protection of passwords, use of software packages, and information on the entity's disciplinary process). *[Reference: 45 C.F.R. §164.530(b(1), (b)(2)(B), (b)(2)(C), & 45 C.F.R. §164.308(a)(5)(i)]*
4.5.2 Documentation	An entity shall document that the training has been provided as required *(see Section 4.4)*. *[Reference: 45 C.F.R. § 164.530(1)(1)(ii)]*

4.6 COMPLAINT PROCESS

Any person may file a complaint with the entity if he/she believes that the requirements of the California Privacy and Security Advisory Board Privacy and Security Guidelines are not being followed.

[References: 45 C.F.R. § 164.530(d)]

4.6.1 Right to File Complaint [New]	A person who believes an entity is not complying with the applicable requirements of these guidelines may file a complaint with the entity that is the subject of the complaint. If the complaint involved a breach of health information, the complaint may be filed with the California Department of Public Health. *[Reference: 45 C.F.R. § 164.530 (d) & California Civil Code §§ 1798.29 and 1798.82, California Health and Safety Code §§ 130200-130205])]*
4.6.2 Complaint Requirements [New]	Complaints under these guidelines must meet the following requirements: *[Reference: [45 C.F.R. § 164.530(d) & 160.306(b)]]*
4.6.2.1 COMPLAINT METHOD	A complaint must be filed in writing, either on paper or electronically. *[Reference: 45 C.F.R. §§ 160.306(b)(1)]*
4.6.2.2 CONTENT	A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable guidelines. *[Reference: 45 C.F.R. §§160.306(b)(2)]*
4.6.2.3 TIMING	A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred. *[Reference: 45 C.F.R. § 160.306(b)(3)]*
4.6.3 Entity Requirements	An entity shall meet the following requirements regarding complaints: *[Reference: 45 C.F.R. § 164.530(d)]*
4.6.3.1 DESIGNATED CONTACT FOR COMPLAINTS	An entity must designate a contact person or office that is responsible for receiving complaints. *[Reference: 45 C.F.R. § 164.530(a)(1)(ii)]*
4.6.3.2 DESIGNATED PROCESS FOR COMPLAINTS	An entity must provide a process for individuals to make complaints concerning the entity's policies and procedures required by these guidelines or its compliance with such guidelines. *[Reference: 45 C.F.R. § 164.530(d)(1)]*
4.6.3.3 REVIEW COMPLAINTS RECEIVED	An entity shall utilize due diligence to investigate all complaints received. *[Reference: California Privacy and Security Advisory Board]*
4.6.3.4 DOCUMENTATION	As required by Section 4.4, an entity must document all complaints received, and their disposition, if any. *[Reference: 45 C.F.R. § 164.530(d)(2)]*
4.6.3.5 COOPERATION	An entity shall cooperate with the California Department of Public Health and the California Office of Health Information Integrity, if either agency undertakes an investigation of the complaint, policies, procedures, or practices of the entity

	to determine it is complying with the applicable provisions of the guidelines. *[Reference: California Health and Safety Code §§ 130200-130205]*

4.7 MITIGATION OF HARM	
4.7.1 Mitigation	An entity shall mitigate, to the extent practicable, any harmful effect that is known to the entity of a use or disclosure of individual health information in violation of its policies and procedures or the requirements of the policies and procedures by the entity or its business associate. [*Reference: 45 C.F.R. § 164.530(f)]*
4.7.2 Mitigation of Security Incidents	An entity shall identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the entity; and document security incidents and their outcomes. *[Reference: 45 C.F.R.§ 164.308(a)(6)]*
4.7.3 Mitigation of Identity Theft	An entity shall have the capability to identify substantiated fraudulent activity within their records and be able to view and/or provide records internally and externally as though the fraudulent activity had not occurred. *[Reference: California Privacy and Security Advisory Board]*

4.8 SANCTION AND ENFORCEMENT POLICY	
4.8.1 Sanctions	An entity shall have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the entity or the California Privacy and Security HIE Guidelines. Entities shall document the sanctions that are applied, if any. *[Reference: 45 C.F.R. § 164.530(e)]*
4.8.2 Breaches	An entity must comply with the breach reporting requirements of California law. *[Reference: California Civil Code §§ 1798.29 & 1798.82, and California Health and Safety Code §§ 1280.15 & 130200-130205]*

5.0 ADMINISTRATIVE CONTROLS

5.1 INFORMATION SECURITY (ORGANIZATION & RESPONSIBILITY)

An entity shall identify the entity's primary security official who is responsible for implementation and compliance to these guidelines. Such official shall be identified in such a way that anyone who might have a security issue or concern may contact that person.

[Reference: 45 C.F.R § 164.308 (a)(2)]

5.1.1 Responsibility and Coordination of Information Security Assets	An entity shall account for information security assets and designate the asset owner. An entity shall assign appropriate security controls for each class or group of information security assets. Implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets. *[Reference: ISO 7.1 Responsibility for Assets]*
5.1.2 Information Security Policy Approvals & Management	An entity shall comply with the following: a) In deciding which security measures to use, an entity shall take into account the following factors: i. The size, complexity, and capabilities of the entity. ii. The entity's technical infrastructure, hardware, and software security capabilities. iii. The costs of security measures. iv. The probability and criticality of potential risks to individual health information. b) This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of these guidelines. *[Reference: 45 C.F.R § 164.316 (a)]*
5.1.3 Applications Inventory	An entity shall identify all operating, database, and application assets (e.g. application software, system software, development tools) that support the exchange and processing of individual health information and document the importance of these assets. An application inventory shall include all information necessary to recover from a disaster, such as, but not limited to, application logging, type of asset, format, location, backup information, license information, and business value. *[Reference: 45 C.F.R. § 164.308 (7)(ii)(E), ISO 7.1.1 Inventory of Assets]*
5.1.4 Isolating Health Care Clearinghouse Functions	If a health care transaction clearinghouse is part of a larger entity, the clearinghouse segment shall protect and isolate individual health information of the clearinghouse from unauthorized access by the larger organization. *[Reference: 45 C.F.R. § 164.308 (a)(4)(ii)(A)]*

5.2 RISK MANAGEMENT & MITIGATION	
An entity shall detect, contain, correct, avert and constrain security incidents. An entity shall perform risk management and mitigation activities at a frequency determined by the entity based on knowledge of activities within their business practices. *[See Section 5.9 (v3) – Frequency of Actions in this document]* *[Reference: 45 C.F.R. § 164.308 (a)(1)(i)]*	
5.2.1 Risk Assessment / Analysis	An entity shall periodically conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of individual health information held, created, processed, transmitted or received by an entity. *[Reference: 45 C.F.R. § 164.308 (a)(1)(ii)(A)]*
5.2.2 Risk Treatment & Management	An entity shall implement security measures sufficient to reduce risks and vulnerabilities to: a) Protect the confidentiality, integrity, and availability of all individual health information the entity creates, receives, maintains, or transmits. b) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. c) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under these guidelines. d) Take steps to ensure compliance with these guidelines by its workforce. *[Reference: 45 C.F.R. §§ 164.308 (a)(1)(ii)(B) & 164.306 (a)]*

5.3 WORKFORCE SECURITY MANAGEMENT	
An entity shall ensure that all members of its workforce have appropriate access to individual health information and to prevent those workforce members who do not have access from obtaining access to individual health information consistent with these guidelines. *[Reference: 45 C.F.R. § 164.308 (a)(3)(i)]*	
5.3.1 Workforce Supervision	An entity shall authorize and/or supervise workforce members who work with individual health information. *[Reference: 45 C.F.R. § 164.308 (a)(3)(ii)(A)]*
5.3.2 Workforce Security (Pre/Post – Employment)	An entity shall determine that the access of an authorized workforce member to individual health information is appropriate and to remove access without delay to individual health information when access is no longer required. *[Reference: 45 C.F.R. §§ 164.308 (a)(3)(ii)(B) & 164.308 (a)(3)(ii)(C)]*
5.3.3 Workforce	An entity shall apply appropriate sanctions against workforce members who fail

Sanctions & Accountability	to comply with the security policies and procedures of the entity. *[Reference: 45 C.F.R. § 164.308 (a)(1)(ii)(C)]*
5.3.4 – Permitted Use of Equipment	An entity shall specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation, including mobile computing devices that can access individual health information. *[Reference: 45 C.F.R. § 164.310 (b)]*

5.4 COMPLIANCE TESTING, AUDIT, & MONITORING

An entity shall take steps to ensure compliance of their systems with these security guidelines. The security of information systems shall be regularly reviewed. Such reviews shall be performed against these guidelines and the technical platforms and information systems shall be audited for compliance with applicable security guidelines.

If any non-compliance is found as a result of the review, managers shall:

a) determine the causes of the non-compliance;

b) evaluate the need for actions to take steps to ensure that non-compliance does not recur;

c) determine and implement appropriate corrective action;

review the corrective action taken.

[Reference: ISO 15.2 Compliance with Security Policies and Standards, and Technical Compliance]

5.4.1 – Activity Review & Monitoring (Logs)	An entity shall regularly review records of activity and monitor information systems that contain individual health information and information security applications, such as audit logs, access reports, and security incident tracking reports for indications of control failure or exploitation of individual health information within information systems. An entity shall use system monitoring to check the effectiveness of controls adopted and to verify conformity to guidelines. An entity shall take actions to remediate, as appropriate. *[Reference: 45 C.F.R. § 164.308 (a)(1)(ii)(D)]*
5.4.2 – Evaluation of Policy and Technical Compliance	An entity shall perform a periodic technical and non-technical evaluation, based initially upon the guidelines implemented and subsequently, in response to guideline changes, environmental or operational changes affecting the security of individual health information. Such evaluations shall be conducted and documented in full or in part as changes indicate, but no less frequently than annually. *[Reference: 45 C.F.R. § 164.308 (a)(8)]*

5.5 SECURITY INCIDENT MANAGEMENT, RESPONSE & DOCUMENTATION

a) An entity shall address security incidents. An entity shall identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the entity; and document security incidents and their outcomes.

b) An entity shall disclose to any resident of California whose unencrypted individual health information was, or is reasonably believed to have been, accessed, acquired, used or disclosed by an unauthorized person following discovery or notification of the breach *[45 C.F.R. § 164.404].* The disclosure shall be made:

   i. In the most expedient time possible,

   ii. Without unreasonable delay [

   iii. No later than five days by a clinic, health facility, agency or hospice licensed by the California Department of Public Health,

   iv. In no case later than 60 days after the discovery of the breach, and

   v. Consistent with the legitimate needs of law enforcement;

      A) The notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation or

      B) Cause damage to national security and

      C) Be made after the law enforcement agency determines that it will not compromise the investigation.

c) An entity shall take measures necessary to determine the scope of the breach and correct offending deficiencies in security controls to prevent a recurrence of the breach of the information system, as appropriate.

[Reference: 45 C.F.R. §§ 164.308 (a)(6)(i) & 164.308 (a)(6)(ii), California Civil Code § 1798, ARRA HITECH Section 13400, California Civil Code § 1798.29, California Health and Safety Code § 1280.15, Federal Register Vol. 74, No. 162, August 24, 2009]

5.6 FREQUENCY OF ACTIONS

Activities required by these guidelines shall be performed at a frequency determined by an entity based on knowledge of activities within their business practices, unless otherwise indicated.

[Reference: California Privacy and Security Advisory Board Security Committee]

6.0 CONTINGENCY PLANNING FOR BUSINESS CONTINUITY

6.1 CONTINGENCY PLANNING

An entity shall have procedures in place to respond to an emergency or other occurrence *(for example, fire, vandalism, system failure, and natural disaster)* that damages systems that contain individual health information, by providing timely access to the necessary individual health information in primary or recovery site facilities in support of emergency recovery operations.

[Reference: 45 C.F.R. §§ 164.310 (a)(2)(i) & 164.312 (a)(2)(ii)]

6.1.1 Applications and Data Criticality Analysis	An entity shall assess the relative criticality of specific applications data in support of other contingency plan components. *[Reference: 45 C.F.R. § 164.308 (a)(7)(ii)(E)]*
6.1.2 Backup and Testing	a) An entity shall create and maintain applications/systems to protect the integrity and availability of individual health information. b) An entity shall implement procedures for periodic testing and revision of contingency plans. *[Reference: 45 C.F.R. §§ 164.308 (a)(7)(ii)(A) & 164.308 (a)(7)(ii)(D)]*
6.1.3 Emergency Operations Plan	An entity shall continue critical business processes that protect and secure individual health information while operating in emergency mode. Such activity shall not impede recovery of systems or endanger patient safety. *[Reference: 45 C.F.R. §§ 164.308 (a)(7)(ii)(C) & 164.310 (a)(2)(ii)]*
6.1.4 Disaster Recovery Plan	An entity shall restore any loss of individual health data, to the extent possible, necessary to its operation or participation in the exchange of health information. *[Reference: 45 C.F.R. § 164.308 (a)(7)(ii)(B)]*
6.1.5 Testing and Revision	An entity shall periodically test and revise their contingency plans. *[Reference: 45 C.F.R. § 164.308 (a)(7)(ii)(D)]*

7.0 FACILITY & EQUIPMENT CONTROLS

7.1 FACILITY ACCESS CONTROLS

An entity shall limit physical access to its information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

[Reference: 45 C.F.R. § 164.310 (a)(1)]

7.1.1 Physical Access Management	a) An entity shall safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft, including procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. b) An entity shall document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks) *[Reference: 45 C.F.R. §§§ 164.310 (a)(2)(ii) & 164.310 (a)(2)(iii) & 164.310 (a)(2)(iv)]*
7.1.2 Communications and Operations Management	a) An entity shall assign responsibilities for the management and operation of all information processing facilities that handle individual health information. b) An entity shall establish formal exchange policies, procedures, and controls to protect the exchange of information using all types of communication facilities. *[Reference: ISO 10.1 Operational Procedures and Responsibilities, 10.8 Exchange of Information]*

7.2 DEVICE AND MEDIA CONTROLS

An entity shall control, administer and maintain a record of:

a) The consignment of hardware and electronic media that contain individual health information and

b) The persons responsible for this activity, and

c) The inventory of such assets.

[Reference: 45 C.F.R. § 164.310 (d)(1)]

7.2.1 Workstation and Equipment Security	An entity shall implement physical and/or technical safeguards for all workstations that access individual health information, to restrict access to authorized users. *[Reference: 45 C.F.R. § 164.310 (c)]*

Controls	
7.2.2 Reuse of Media	An entity shall implement procedures for removal of individual health information from electronic media before the media are made available for re-use. *[Reference: 45 C.F.R. § 164.310 (d)(2)(ii), Federal Register / Vol. 74, No. 79 / Monday, April 27, 2009Pages 19006-19010]*
7.2.3 Disposal of Media	a) An entity shall utilize a method that best meets the entity's business practices and protects the security of individual health information for final disposition of individual health information, hardware, and/or electronic media on which the individual health information is stored. b) Individual health information is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies: i. Electronic individual health information: A) Has been encrypted [as specified in the HIPAA Security Rule 45 C.F.R. § 164.312 (a)(2)(iv)] by 'the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key,'' and B) Such confidential process or key that might enable decryption has not been breached. ii. The media on which the individual health information is stored or recorded have been destroyed in one of the following ways: A) Paper, film, or other hard copy media have been shredded or destroyed such that the individual health information cannot be read or reconstructed. Redaction is specifically excluded as a means of data destruction. B) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800–88, Guidelines for Media Sanitization. *[Reference: 45 C.F.R. § 164.310 (d)(2)(i), Federal Register / Vol. 74, No. 79 / Monday, April 27, 2009 Pages 19006-19010]*

7.3 TECHNICAL CONTROLS

An entity shall protect individual health information in information systems as specified in the guidelines.

[Reference: 45 C.F.R. § 164.312(a)]

7.3.1 Activity	An entity shall monitor log-in attempts, reporting discrepancies, and take

Monitoring Controls	actions to remediate, as appropriate. *[Reference: 45 C.F.R. § 164.308 (a)(5)(ii)(C)]*
7.3.2 Operating System (OS) & Database Hardening / Patch Management	An entity shall comply with the following as necessary for the protection of individual health information: a) Apply patches or use other appropriate mechanisms b) Update the operating system (OS) and databases c) Harden and configure the OS and databases to address security vulnerabilities d) Install and configure necessary security controls e) Test the security of the OS and databases to ensure that the previous steps address known security issues *[Reference: NIST SP 800-123 (Section 4) – Securing the Server Operating System]*
7.3.3 Malicious Code Protection	An entity shall take appropriate steps to protect against malicious software. In addition, an entity shall incorporate a mechanism to detect, and immediately report malicious software to the primary security official. *[Reference: 45 C.F.R. § 164.308 (a)(5)(ii)(B)]*
7.3.5 Email & Messaging Security	An entity shall safeguard electronic mail and messaging containing individual health information, including, but not limited to: a) Protecting messages from unauthorized access, modification or disclosure; b) Correctly addressing and transporting the message; c) Securing general reliability and availability of the service; d) Complying with other legal considerations, for example requirements for electronic signatures and encryption; e) Obtaining appropriate approval prior to using external public services such as instant messaging or file sharing; and f) Establishing levels of access control and encrypt individual health information when transmitting over publicly accessible networks. *[Reference: NIST SP 800-45 v2 Guidelines on Electronic Mail Security, ISO 10.8.4 Electronic Messaging]*
7.3.6 Audit Controls & Considerations	An entity shall implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use individual health information. *[Reference: 45 C.F.R. § 164.312 (b), NIST SP 800-123 (Section 6.4.2) Penetration Testing]*

7.4 NETWORK SECURITY MANAGEMENT	
An entity shall protect the networks and infrastructures that maintain or transmit individual health information. *[Reference: ISO 10.6 Network Security Management*	
7.4.1 Perimeter Controls and Management	An entity shall identify and include, or reference, security features, service levels, and management requirements of all network services in any network services agreement, whether these services are provided in-house or outsourced. Network services include the provision of connections, private network services, and value added networks and managed network security solutions such as firewalls and a system to detect intrusion. *[Reference: ISO 10.6.2 Security of Network Services]*
7.4.2 Unsecured IHI Loss Prevention	An entity shall take reasonable steps to prevent the unauthorized removal or transmission of individual health information from its information systems, including data leakage, laptop or flash drive loss, etc. *[Reference: Federal Register / Vol. 74, No. 79 / Monday, April 27, 2009 Pages 19006-19010]*
7.4.3 Intrusion Detection	An entity shall implement an internal system to detect, document and report on potential intrusion attempts and identify security policy violations. *[Reference: NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)]*
7.4.4 Web Services	An entity shall secure all Web services to protect individual health information to include access controls, data integrity, risk management and mitigation, contingency planning and email security. *[Reference: NIST SP 800-95 Guide to Secure Web Services]*
7.4.5 Consistent Time	An entity shall take steps to ensure clocks of all relevant information processing systems within an organization or security domain are synchronized using Healthcare Information Technology Standards Panel (HITSP)/T16 Consistent Time Transaction (http://wiki.hitsp.org/docs/T16/T16-1.html) *[Reference: HITSP T16 Consistent Time Transaction, ISO 10.10.6 Clock Synchronization]*

8.0 DATA PROTECTION AND USER ACCESS CONTROLS	
8.1 Access Controls	An entity shall utilize identity management, authentication, and authorization mechanisms to ensure that only authorized users have access to information systems. *[45 C.F.R. § 164.312 (a)]*

8.1.1 Identity Management (Internal)	An entity shall assure that the person is the person claimed *(verification) [See Guideline 4.3 Verification of Identity]* a) An entity shall issue a user identifier, or identity certificate and/or token *(password, hard token, soft cryptographic token or one-time password device tokens, etc.),* to the verified person, as appropriate. b) An entity shall be responsible for any health data access rights assigned to the authorized person based on their qualifications and role. c) An entity shall manage all stages in the life cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. *[Reference: NIST SP 800-63 (Section 6.3.1) Requirements per Assurance Level, ISO 11.2 User Access Management]*
8.1.2 Single Entity Authentication (Non-Federated)	a) An entity shall authenticate each authorized user's identity prior to providing access to individual health information. b) An entity shall assign a unique name and/or number for identifying and tracking user identity and implement procedures to verify that a person or entity that is seeking access to individual health information is the one claimed. c) An entity shall authenticate each user to the level of authorized access that complies with the entity's level of trust agreement with the external exchange entity. d) An entity shall authenticate users attempting to access individually identifiable health information remotely from an unsecured location or device, shall require NIST Level 3 authentication in which the data requester must establish two factors of authentication. [*See NIST SP 800-63 Rev-1*] *[Reference: 45 C.F.R. §§ 164.312 (a)(2)(i) & 164.312 (d), NIST SP 800-63 Rev 1 Electronic Authentication Guideline, OMB Safeguarding Against and Responding to the Breach of Personally Identifiable Information M 07-16]*
8.1.3 Authentication Across Multiple Entities (Federated)	a) If an entity is participating in a trust network health information exchange, i. The trust network shall manage entity authentication for those participating on the trust network, and ii. An entity shall manage user authentication only for those entities participating on the trust network. b) If the user authentication process is across multiple systems or entities, an entity shall implement the agreed upon authentication process among the participants in the trust network. c) An entity participating in the trust network shall implement a trust agreement. *[See Guideline 4.9 Contracts and Agreements]* *For example, an entity may use an Interconnections Security Agreement (ISA) and Memorandum of Understanding (MOU) in accordance with NIST SP 800-47 Federal Security Guide for Interconnecting Information*

	Technology Systems, unless such requirement has been superseded by implementation of the national Data Use and Reciprocal Support Agreement (DURSA). d) The entity shall adopt an authentication solution that incorporates the authorization requirement of these guidelines. *(See Guideline 8.1.4 (v3) Authorization & Access Control.)* *[Reference: California Privacy and Security Advisory Board Security Access Controls Comparative Analysis]*
8.1.4 Authorization & Access Control	An entity shall use the following access control attributes to determine if a user is authorized to access requested information in a way that corresponds to, and is compliant with, the data use agreements governing such access and as it aligns with state requirements: a) Data Source; b) Entity of Requestor; c) Role of Requestor; d) Use of Data; e) Sensitivity of Data; f) Form of Data (or, how the data is provided); g) Consent Directives of the Data Subject An entity that acts as a data requestor shall execute the authorization process at the location agreed upon in the data use agreements governing that exchange. The data requestor shall pass the authentication and authorization to the data supplier as a single message if so designated by the data use agreement. [*Reference:* California Privacy and Security Advisory Board *Security Access Controls Comparative Analysis*
8.1.5 Password Management	An entity shall require passwords to be created, changed periodically, safeguarded, and of sufficient strength to protect the individual health information, as appropriate, unless the entity uses other comparable authentication methods. *[Reference: 45 C.F.R. § 164.308 (a)(5)(ii)(D)]*
8.1.6 Session Controls (Automatic Logoff)	An entity shall determine the amount of time a session may be inactive before termination. An entity shall terminate electronic session after the established time of inactivity. *[Reference: 45 C.F.R. § 164.312 (a)(2)(iii)]*

8.2 DATA ASSURANCE
a) An entity shall protect individual health information from unauthorized alteration or destruction.

b) An entity shall implement technical security measures to protect against unauthorized access to individual health information that is being transmitted over an electronic communications network. *[Reference: 45 C.F.R. §§ 164.312 (c)(1) & 164.312 (e)(1)]*	
8.2.1 Encryption and Cryptographic Controls	An entity shall implement a mechanism to provide the ability to encrypt and decrypt where appropriate, to protect individual health information. *[Reference: 45 C.F.R. § 164.312 (a)(2)(iv)]*
8.2.2 Integrity Controls (including non-repudiation)	An entity shall implement security measures to safeguard electronically transmitted individual health information being improperly modified without detection until disposed. This includes implementation of electronic mechanisms to corroborate that individual health information has not been altered or destroyed in an unauthorized manner. *[Reference: 45 C.F.R. §§ 164.312 (e)(2)(i) & 164.312 (c)(2)]]*

9.0 DEFINITIONS

Access (Privacy)	An individual's right to inspect and obtain a copy of his/her individual health information maintained by an entity. *[based on 45 C.F.R. §164.524]*
Access (Security)	The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. *[45 C.F.R. § 164.304]*
Access Control (Technical)	The policies, rules, or deployment mechanisms which prevent unauthorized access, use, disclosure or transmission of information or information systems by controlling access to networks, computer devices, computer applications, programs or data. *[Health Information Technology Standards Panel and Health Information Security and Privacy Collaboration]*
Accountability	Ensuring that the actions of an individual or entity, and the permission for the action, may be traced to that individual or entity and the individual or entity that approved permission for the action. *[Based upon Health Information Security and Privacy Collaboration]*
Addendum	A 250 word-limited addition an individual can provide to correct or amend his/her individual health information. *[California Health and Safety Code § 123111]*
Administrative Safeguards (Security)	Actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic individual health information and to manage the conduct of the entity's workforce in relation to the protection of that information. *[45 C.F.R. § 164.103]*
Amend or Amendment	Direct changes made to an existing record that affects the data associated with the 'current' version of a record. The identifier associated with the record remains the same, though a copy of the original version is retained and can be

	accessed by querying for the history of the record. There are usually limitations on what amendments can be made for a given type of record, and the specifics of those amendments. In general, amendments are supported for records where the information associated with the record is frequently subject to change. *[Certification Commission for Health Information Technology]*
Asset Owner	An individual or entity (e.g., data custodian, data host) that has management responsibility for controlling the production, development, maintenance, use and security of the assets. [*ISO/IEC 27002:2005, Section 7.1 Responsibility for Assets]*
Audit Log	Audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function. Audit records typically result from activities such as transactions or communications by individual people, systems, accounts or other entities. *[Wikipedia]*
Authentication	a) Corroboration that a person is the one claimed. *[45 C.F.R. § 164.103]* b) Verifying the identity of an individual, originator, user, terminal, workstation, process, or device to determine an entity's right to access specific categories of information, and a measure designated to protect against fraudulent access, use, disclosure, alteration, transmission or deletion before allowing access to an information system by verifying through reliable security identification of subjects incorporating identifiers and authenticators. *[California Privacy and Security Advisory Board]*
Authorization (Privacy)	Documented permission granted by an individual in a form that adheres to the Guideline authorization requirements whereby an individual provides permission for the use or disclosure of his/her individual health information. *[California Privacy and Security Advisory Board]*
Authorization (Security)	A system established to grant access to confidential information, establishes the level of access an individual or entity has to a data set and includes a management component, i.e., an individual or individuals must be designated to authorize access and manage access once access is approved. *[Health Information Security and Privacy Collaborative]*
Authorization Arbitration	A process of considering all relevant attributes of information requests that may affect the decision on what "protected" information may be provided in response to a data request from an authorized requestor. *[California Privacy and Security Advisory Board]*
Authorized User	Any person or entity that is authorized to request, access, use or disclose individual health information utilizing an electronic health information exchange. *[California Privacy and Security Advisory Board]*
Breach	Unauthorized acquisition of individual health information that compromises the security, confidentiality, or integrity of information maintained by a person or business. *[California Civil Code § 1798.82(d)]*

Business Associate	A person or entity who: a) On behalf of a covered entity in a capacity other than that of a member of the entities' workforce performs or assists in the performance of: i. A function or activity involving the use or disclosure of individual health information, including claims processing or administration, data analysis, processing, or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or ii. Any other function or activity regulated by 45 C.F.R. Parts 160, 162, & 164 (HIPAA) b) Provides, other than in the capacity of a member of the workforce of such entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such entity, where the provision of the service involves the disclosure of individual health information from such entity from another business associate of such entity to the person. c) An entity may be a business associate of another entity. *[45 C.F.R. § 160.103]*
Chain of Trust (Trust Network)	A group of service providers that share linked identities and have pertinent business agreements in place regarding how to do business and interact with each identity. Once a user has been authenticated by a Chain of Trust identity provider, that individual can be easily recognized and take part in targeted services from other service providers within that Chain of Trust. *[Liberty Alliance]*
Consent	See HIEconsent.
Correctional Institution	Correctional institution means any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial. . *[45 C.F.R. §164.501]*
Direct Treatment Relationship	A direct treatment relationship is between an individual and a health care provider in which the primary health care provider provides direct treatment to the individual. *[Based on the definition of indirect treatment relationship in 45 C.F.R. § 164.501]*
Disclose / Disclosure	Any release, transfer, dissemination, or other communication, of all or any part of any individual health information record orally, or in any manner, to another entity, including one entity accessing the individual health information record of another entity. *[California Privacy and Security Advisory Board]*

Electronic Health Information Exchange *(eHIE)*	The electronic movement of health related data and information among organizations. *[California Privacy and Security Advisory Board]*
Electronic Health Record *(EHR)*	An electronic record of health-related information about an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one health care organization. *[National Alliance for Health Information Technology]*
Electronic Media	Electronic storage media including memory devices in computers (hard drives) and any other removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory cards; or Transmission media used to exchange information already in electronic storage media. Transmission media includes, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to the collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission. *[45 C.F.R. § 160.103]*
Emancipated Minor	Person under the age of 18 years is an emancipated minor if any of the following conditions is satisfied: (a) The person has entered into a valid marriage, whether or not the marriage has been dissolved. (b) The person is on active duty with the armed forces of the United States. (c) The court has issued a declaration of emancipation. *[Reference: California Family Code §§ 7002 &7122]*
Employer	The person for whom an individual performs or performed any service, of whatever nature, as the employee of such person, except that— a) If the person for whom the individual performs or performed the services does not have control of the payment of the wages for such services, the term "employer" means the person having control of the payment of such wages, and b) In the case of a person paying wages on behalf of a nonresident alien individual, foreign partnership, or foreign corporation, not engaged in trade or business within the United States, the term "employer" means such person. *[As defined in 26 USC 3401(d)]; [45 C.F.R. § 160.103]*
Encryption	Use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

	[HIPAA]
Entity	A person, corporation, association, partnership or other legal entity in possession of individual health information, other than an individual in possession of his/her individual health information. For example, physician, hospital, provider, health plan, clearinghouse, health information organization, regional health information organization, clinic, etc. *[California Privacy and Security Advisory Board]*
Health Care	Care, services, or supplies related to the health of an individual. Health care includes, but is not limited to: a) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and b) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription. *[45 C.F.R. § 160.103]*
Health Care Clearinghouse	A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions: a) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction. b) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity. *[45 C.F.R. § 160.103]*
Health Care Operations	The following activities of a healthcare provider or health plan are healthcare operations: a) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; b) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, accreditation, certification, licensing, or credentialing activities; c) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; and limited to: i. Business planning and development, such as conducting cost-

management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

ii. Business management and general administrative activities of the entity, including, but not limited to:

A) Management activities relating to implementation of and compliance with the requirements of these guidelines;

B) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

C) Resolution of internal grievances;

D) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

E) Consistent with the applicable requirements of 45 C.F.R. §164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

iii. Population-based activities relating to reducing health care costs;

iv. Related functions that do not include treatment, such as disease management under Civil Code § 56.10(c)(17);

v. Conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals;

vi. Underwriting limited to Civil Code §§ 56.10(c)(9) and 56.10(c)(11).

[Reference: 45 C.F.R. §§ 164.502(a)(1)(ii) & 164.506(c)(3), California Civil Code § 56.10(c)(3) & § 56.10(c)(4) & § 56.10(c(5)]

Health Care Provider

Health care provider means:

a) A provider of services as defined in section 1861(u) of the Social Security Act (42 USC. 1395x(u)),

b) A provider of medical or other health services as defined in section 1861(s) of the Social Security Act (42 USC. 1395x(s)), and

c) Any other person who furnishes or bills and is paid for health care in the normal course of business. *[45 C.F.R. § 142.103]*

Health Information

Any information, whether oral or recorded in any form or medium, that:

a) Is created or received by, including but not limited to, a health care provider, health plan, public health authority, employer, life insurer, school or university, health care clearing house, personal health record, or health

	information organization; and b) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual [*45 C.F.R. §160.103*]
Health Information Exchange *(HIE)*	The electronic movement of health-related information among organizations according to nationally recognized standards. *[National Alliance for Health Information Technology]*
HIEconsent	Permission granted by an individual or an authorized person that allows the provider, agency, or organization to exchange individual health information via an electronic health information exchange. The authorized person may be the subject of the information or they may be a designated representative such as a parent or guardian. [California Privacy and Security Advisory Board]
Health Information Organization *(HIO)*	An organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards. *[National Alliance for Health Information Technology]*
Health Information Technology *(HIT)*	Health information technology means hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information. [42 USC *§* 300jj(5)]
Health Oversight Agency	An agency or authority of the United States, a State, a territory, or political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether privacy or public) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant. *[45 C.F.R. § 164.501]*
Health Plan	An individual or group plan that provides, or pays the cost of, medical care. *[45 C.F.R. § 160.103]*
HIEconsent	Permission granted by an individual or an authorized person that allows the provider, agency, or organization to exchange individual health information via an electronic health information exchange. The authorized person may be the subject of the information or they may be a designated representative such as a parent or guardian. [California Privacy and Security Advisory Board]
HIPAA	The Health Insurance Portability and Accountability Act passed by Congress in 1996 to ensure that an individual's health insurance would not stop when they changed employment. It also provided the Administrative Simplification to adopt national standards for electronic health care transactions. At the same time

	Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of federal privacy and security protections for individually identifiable health information. HIPAA regulations may be found at 46 C.F.R. parts 160, 162, 163m and 164. *[HISPC]*
Identity (Privacy)	The collective set of characteristics by which a person is definitively recognizable or known. *[California Privacy and Security Advisory Board]*
Identity (Security)	A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example an address, or some unique identifier such as an employee or account number) to make the complete name unique. *[NIST 800-63-1]*
Identity Access Management	Set of services to include authentication, user provisioning (UP), password management, role matrix management, enterprise single sign-on, enterprise access management, federation, virtual and meta-directory services, and auditing. *[Certification Commission for Health Information Technology]*
Indirect Treatment Relationship	A relationship between an individual and a health care provider in which: a) The health care provider delivers health care to the individual based on orders of another health care provider; and b) The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly through another health care provider, who provides the services or products or reports to the individual. *[45 C.F.R. § 164.501]*
Individual	The person who is the subject of the individual health information; generally the patient. *[45 C.F.R. § 164.501]*
Individually Identifiable	Information for which there is a reasonable basis to believe that such information, alone or in combination with other reasonably available information, could reveal the individual's identity. *[California Privacy and Security Advisory Board]*
Individual Health Information	Health information obtained from or about an individual that contains information that identifies the individual of whom the information concerns. *[California Privacy and Security Advisory Board]*
Information Security Event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant. *[ISO/IEC TR 18044:200 4]*
Integrity	The state in which data or information have not been altered or destroyed in an unauthorized manner. *[45 C.F.R. § 164.304]*
Knowledgeable HIEconsent	An HIEconsent to the collection, request, use or disclosure of an individual's health information is knowledgeable if it is reasonable in the circumstances to

	believe that the individual knows: a) The purposes of the collection, use or disclosure, as the case may be. b) That the individual may give or withhold HIEconsent. *[Canada Personal Health Information Protection Act, 2004, Part III, 18]*
Law Enforcement Official	An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a Stat or territory, or an Indian tribe, who is empowered by law to: a) Investigate or conduct an official inquiry into a potential violation of law, or b) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law. *[45 C.F.R. § 164.501]*
Licensed Health Care Professional	Any person licensed or certified pursuant to Division 2 *(commending with Section 500)* of the California Business and Professions Code, the Osteopathic Initiative Act or the Chiropractic Initiative Act, or Division 2.5 *(commencing with Section 1797)* of the California Health and Safety Code. *[Civil Code Section 56.05(e)]*
Limited Data Set	A limited data set is individual health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: a) Names; b) Postal address information, other than town or city, state, and zip code; c) Telephone numbers; d) Fax numbers; e) Electronic mail addresses; f) Social security numbers; g) Medical record numbers; h) Health plan beneficiary numbers; i) Account numbers; j) Certificate/license numbers; k) Vehicle identifiers and serial numbers, including license plate numbers; l) Device identifiers and serial numbers; m) Web Universal Resource Locators (URLs); n) Internet Protocol (IP) address numbers; o) Biometric identifiers, including finger and voice prints; and p) Full face photographic images and any comparable images. *[Reference: 45 C.F.R. § 164.514(e)(2)]*
Marketing	Marketing is to make a communication about a product or service that encourages recipients of the communication to purchase or use the product, brand or service.

	Marketing does not include the following: Communication that is without remuneration, either direct or indirect, and is for any of the following purposes: a) For treatment of the individual, b) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual, or c) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: i. Replacement of, or enhancements to, a health plan, or ii. Health-related products or services available only to a health plan enrollee that adds value to, but are not part of, a plan of benefits. *[45 C.F.R. § 164.501, 164.506(a)(3), HITECH, Section 13406, California Civil Code § 56.05 & 56.10(d)]*
Mask or Masking	A process of restricting access to or transfer of individual health information. Typically masking is applied at the data source and may be overridden, as permitted by law, by the accessing custodian (e.g., in an emergency situation). *[Certification Commission for Health Information Technology]*
Mental Health Records	Patient records, or discrete portions thereof, specifically related to evaluation or treatment of a mental disorder. Includes but is not limited to all alcohol and drug abuse records. *[Health and Safety Code section 123105(b)]*
Minimum Necessary	The minimum amount of individual health information that is necessary to meet the intended purpose of the request, collection, use, or disclosure. *[45 C.F.R. §§ 164.502(b) & 164.514(d)]*
Minor	A minor is an individual who is under 18 years of age. The period of minority is calculated from the first minute of the day on which the individual is born to the same minute of the corresponding day completing the period of minority. *[Reference: California Family Code §§ 6500]*
Network Service Agreement	A security agreement necessary to obtain particular services, such as security features, service levels, and management requirements. The agreement should ensure that network service providers include the provision of connections, private network services, and value-added networks and managed network security solutions such as firewalls and intrusion detection systems. *[ISO/IEC 27002:2005 Section 10.6.2 Security of Network Services]*
Notice of Privacy Practices *(Privacy Notice)*	A document provided to patients that explains an entities privacy practices and how information about an individual's health information may be shared. *[California Privacy and Security Advisory Board]*
Opt In with Restrictions	An alternative where an individual may decide to include their individual health information, or part of their individual health information in the HIE system. *[California Privacy and Security Advisory Board]*

Opt Out	An alternative where an individual may decide not to allow access or disclosure of their individual health information which is in the HIE system. *[California Privacy and Security Advisory Board]*
Organized Health Care Arrangement	a) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider; b) An organized system of health care in which more than one covered entity participates, and in which the participating covered entities: i. Hold themselves out to the public as participating in a joint arrangement; and ii. Participate in joint activities that include at least one of the following: A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf; B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk. c) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan; d) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or e) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans. *[45 C.F.R. § 164.501]*
Payer	Insurers, including health plans, self-insured employer plans, and third-party administrators, providing health care benefits to enrolled members and reimbursing provider organizations. As part of this role, they provide information on eligibility and coverage for individual consumers, as well as claims-based information on consumer medication history. Case management or disease management may also be supported.. [HISPC]
Payment	a) The activities untaken by:

	i. A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or ii. A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and b) These activities relate to the individual to whom health care is provided and include, but are not limited to: i. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; ii. Risk adjusting amounts due based on enrollee health status and demographic characteristics; iii. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing' iv. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; v. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and vi. Disclosure of consumer reporting agencies of any of the following individual health information related to the collection of premiums or reimbursement: A) Name and address; B) Date of birth; C) Social security number; D) Payment history; E) Account number; and F) Name and address of the health care provider and/or health plan. *[45 C.F.R. § 164.501]*
Person	A natural person, trust or estate, partnership, corporation, limited liability company, firm, association, professional association or corporation, or other entity, public or private. *[45 C.F.R. § 160.103 & Civil Code section 1798.3(fc)]]*
Personal Health Record *(PHR)*	An electronic record of health-related information of an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual. [National Alliance for Health Information Technology]
Personal Representative	a) A parent or guardian of a minor who is a patient, b) Conservators, guardians, or agents (pursuant to Probate Code § 4607) of a

	person or adult patient, or c) The executor, administrator, beneficiary (as defined in Section 24 of the Probate Code or personal representative as defined in Section 58 of the Probate Code), or representative of a deceased person. *[California Privacy and Security Advisory Board]*
Physical Safeguards	Measures, policies and procedures to protect an entity's electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. *[45 C.F.R. § 164.304]*
Psychotherapy Notes	Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversations during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes: a) Medication prescriptions and monitoring, b) Counseling session start and stop times, c) The modalities and frequencies of treatment furnished, d) Results of clinical tests, and e) Any summary of the following items: i. Diagnosis, ii. Functional status, iii. The treatment plan, iv. Symptoms, v. Prognosis, and vi. Progress to date. *[45 C.F.R. § 164.501]*
Public Health	Program(s) that promote, maintain, and conserve the public's health by providing health services to individuals and/or by conducting research, investigations, examinations, training, and demonstrations. Public health services may include but are not limited to the control of communicable diseases, immunizations, maternal and child health programs, sanitary engineering, sewage treatment and disposal, sanitation inspection and supervision, water purification and distribution, air pollution control, garbage and trash disposal, and the control and elimination of disease-carrying animals and insects. *[U.S. General Services Administration Website]*
Public Health Authority	An agency or authority of the United States, a State, a territory, or political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate. *[45 C.F.R. § 164.501]*

Required by Law	A mandate contained in law that compels an entity to make a use or disclosure of protected health information and that is enforceable in a court of law. "Required by law" includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits. *[45 C.F.R. § 164.103]*
Research	Systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalized knowledge. *[45 C.F.R. § 164.501]*
Safeguards	Measures that protect the security of health information. [Health Information Security and Privacy Collaborative]
Security	Encompasses all administrative, physical, and technical safeguards in an information system. Includes processes, practices and software that secure health information from unauthorized access, ensuring that the information is not altered and that it is accessible when needed by those authorized. *[45 C.F.R. § 164.304] & Health Information Security and Privacy Collaborative]*
Security Assets	Information, software assets, physical assets, services and people. *[International Organization for Standardization (ISO)/IEC 27002:2005, Section 7.1 Responsibility for Assets]*
Security Incident	Attempted or successful unauthorized access, use, disclosure, modifications, or destruction of information or interference with system operations in an information system. *[45 C.F.R. § 164.304]*
Sensitive Information	Health information which is specifically protected by laws separate from general health information. *[California Privacy and Security Advisory Board]*
Technical Safeguards	Technology and policy and procedures for its use that protect individual health information and control access to it. *[45 C.F.R. § 164.304]*
Transmit/ Transmission	A process to transfer data from point-to-point over a physical point-to-point or point-to-multipoint communication channel. For purposes of the California Privacy and Security Board Guideline scope, transmit does not apply to a midpoint service that only provides a data pass-through function that does not access data content. *[California Privacy and Security Advisory Board]*
Treatment	Provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers related to a patient; or the referral of a patient for health care from one health care provider to another. *[45 C.F.R. § 164.501]*

Treatment Relationship	A treatment relationship includes: a) The relationship between a health care provider who provides direct treatment to the individual. b) The relationship between the health care provider who delivers health care to the individual based on the orders of the primary health care provider, or c) When the health care provider who provides services, products, reports of diagnosis, or results reported directly to the primary health care provider who then provides such items to the individual. *[California Privacy and Security Advisory Board and based on the definition of indirect treatment relationship in 45 C.F.R. § 164.501]*
Unauthorized Access	The act of gaining access to a network, system, application, health information or other resource without permission. *[Health Information Security and Privacy Collaborative]*
Unauthorized Disclosure	The act of exposing, releasing, or displaying health information to those not authorized to have access to the information. *[Health Information Security and Privacy Collaborative]*
Use	With respect to the sharing of individual health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains or transmits such information. *[45 C.F.R. § 160.103]*
Verification of Identity	Process by which the identity of an individual, authorized representative or user is verified. *[45 C.F.R. § 164.514(h)(1)]]*